Document made available under the Patent Cooperation Treaty (PCT)

International application number: PCT/US2005/045440

International filing date: 16 December 2005 (16.12.2005)

Document type: Certified copy of priority document

Document details: Country/Office: US
Number: 60/636,741
Filing date: 16 December 2004 (16.12.2004)

Date of receipt at the International Bureau: 15 February 2006 (15.02.2006)

Remark: Priority document submitted or transmitted to the International Bureau in compliance with Rule 17.1(a) or (b)

1425736

THE UNITED STATES OF AMERICA

TO ALL TO WHOM THESE PRESENTS SHALL COME:

UNITED STATES DEPARTMENT OF COMMERCE

United States Patent and Trademark Office

February 08, 2006

THIS IS TO CERTIFY THAT ANNEXED HERETO IS A TRUE COPY FROM THE RECORDS OF THE UNITED STATES PATENT AND TRADEMARK OFFICE OF THOSE PAPERS OF THE BELOW IDENTIFIED PATENT APPLICATION THAT MET THE REQUIREMENTS TO BE GRANTED A FILING DATE.

APPLICATION NUMBER: *60/636,741*
FILING DATE: *December 16, 2004*
RELATED PCT APPLICATION NUMBER: *PCT/US05/45440*

THE COUNTRY CODE AND NUMBER OF YOUR PRIORITY APPLICATION, TO BE USED FOR FILING ABROAD UNDER THE PARIS CONVENTION, IS *US60/636,741*

Certified by

Jon W. Dudas

Under Secretary of Commerce
for Intellectual Property
and Director of the United States
Patent and Trademark Office

PTO/SB/16 (04-04)
Approved for use through 07/31/2006. OMB 0651-0032
U.S. Patent and Trademark Office; U.S. DEPARTMENT OF COMMERCE
Under the Paperwork Reduction Act of 1995, no persons are required to respond to a collection of information unless it displays a valid OMB control number.

PROVISIONAL APPLICATION FOR PATENT COVER SHEET

This is a request for filing a PROVISIONAL APPLICATION FOR PATENT under 37 CFR 1.53(c).

Express Mail Label No. EV 517424183 US

INVENTOR(S)

Given Name (first and middle [if any])	Family Name or Surname	Residence (City and either State or Foreign Country)
WILLIAM	DOUGLASS	SANTA CLARA, CA

Additional inventors are being named on the 1 *separately numbered sheets attached hereto*

TITLE OF THE INVENTION (500 characters max)

HIGH PERFORMANCE WLAN MOBILE ADAPTER

Direct all correspondence to: **CORRESPONDENCE ADDRESS**

☑ Customer Number: 021498

OR

☐ Firm or Individual Name

Address

Address

City | State | Zip

Country | Telephone | Fax

ENCLOSED APPLICATION PARTS *(check all that apply)*

☑ Specification *Number of Pages* 90

☐ Drawing(s) *Number of Sheets*

☐ Application Data Sheet. See 37 CFR 1.76

☐ CD(s), Number

☑ Other (specify) TITLE PAGE, POSTCARD

Alternate wireless sheet - 3 pgs.

METHOD OF PAYMENT OF FILING FEES FOR THIS PROVISIONAL APPLICATION FOR PATENT

☐ Applicant claims small entity status. See 37 CFR 1.27.

☐ A check or money order is enclosed to cover the filing fees.

☑ The Director is hereby authorized to charge filing fees or credit any overpayment to Deposit Account Number: 50-0210

☐ Payment by credit card. Form PTO-2038 is attached.

FILING FEE Amount ($): $200.00

The invention was made by an agency of the United States Government or under a contract with an agency of the United States Government.

☑ No.

☐ Yes, the name of the U.S. Government agency and the Government contract number are:

Respectfully submitted,

SIGNATURE

TYPED or PRINTED NAME PAUL C. HASHIM

TELEPHONE 972-684-7886

Date 16 DECEMBER 2004

REGISTRATION NO. 31,618 *(if appropriate)*

Docket Number: 17517RRUS01P

USE ONLY FOR FILING A PROVISIONAL APPLICATION FOR PATENT

This collection of information is required by 37 CFR 1.51. The information is required to obtain or retain a benefit by the public which is to file (and by the USPTO to process) an application. Confidentiality is governed by 35 U.S.C. 122 and 37 CFR 1.14. This collection is estimated to take 8 hours to complete, including gathering, preparing, and submitting the completed application form to the USPTO. Time will vary depending upon the individual case. Any comments on the amount of time you require to complete this form and/or suggestions for reducing this burden, should be sent to the Chief Information Officer, U.S. Patent and Trademark Office, U.S. Department of Commerce, P.O. Box 1450, Alexandria, VA 22313-1450. DO NOT SEND FEES OR COMPLETED FORMS TO THIS ADDRESS. **SEND TO: Commissioner for Patents, P.O. Box 1450, Alexandria, VA 22313-1450.**

If you need assistance in completing the form, call 1-800-PTO-9199 and select option 2.

PROVISIONAL APPLICATION COVER SHEET
Additional Page

PTO/SB/16 (10-01)
Approved for use through 10/31/2002. OMB 0651-0032
U.S. Patent and Trademark Office; U.S. DEPARTMENT OF COMMERCE

Docket Number	17517RRUS01P

INVENTOR(S)/APPLICANT(S)

Given Name (first and middle [if any])	Family or Surname	Residence (City and either State or Foreign Country)
WILLIAM	DOUGLASS	SANTA CLARA, CA
TOM	JENCZ	SANTA CLARA, CA
LISA	SCHWARTZ	SANTA CLARA, CA
FRANK	BURKE	SANTA CLARA, CA
IOANNIS	APOSTOLAKOS	SANTA CLARA, CA

WARNING: Information on this form may become public. Credit card information should not be included on this form. Provide credit card information and authorization on PTO-2038.

PROVISIONAL FILING

HIGH PERFORMANCE WLAN MOBILE ADAPTER

INVENTOR:

William R. Douglass
Tom Jencz
Lisa Schwartz
Frank Burke
Ionnis Apostolakos

16 December 2004

Docket Number
17517RRUS01P

High Performance WLAN Mobile Adapter

Fundamental Specification and Design Document
Custom Client Driver Modifications

Revision Log		
Rev.	**Description**	**Author**
1.01	First Draft based on BobO's ACE document and 3/5 conference call with JohnB, Tarek, Darwin, Scott BobO, PaulD and GreggD	Bob Friday
1.02	Updated Handoff Section	Bob Friday
1.03	Added more detail to the handoff section	Bob Friday
1.04	Incorporated Scott's feedback	Bob Friday
1.05	Incorporated 3/12/04 Review Comments and BobOs comments and changes	Bob Friday
1.06	Incorporated 3/15/04 review comments and changes	Bob Friday
1.07	Incorporated BobO's and Larry's comments/changes	Bob Friday
1.08	Reviewed and Incorporated BobO's comments	Bob Friday
1.09	Added CoChannel Interference Details, 2201 Pwr Consumption, Review of BobO's comments	Bob Friday
1.10	BobO's 3/22 meeting notes, BobO's IE changes, Paul D's AES tasks	Bob Friday
1.11	Added Custom Client Test Plan Chapter	Bob Friday
1.12	Added more test plan detail	Bob Friday
1.13	Added GreggD's comments	Bob Friday
1.14	Added Load Balancing Details	Bob Friday
1.15	Updated Design Doc to reflect modification during tests	
1.16	Updated the design to handle the cases 1- Added to state to handle the case when we can not find any APs above the threshold to stop excessive probing 2- Make sure we have current information on our current AP when making handoff decisions. 3- Add a disconnect timeout to state 7 that notifies the OS that the network is disconnected 4- Have the client advertise that it will be doing load sharing	Bob Friday
1.17	Modified state 3 to ensure we end with a traffic mode to get any packets that maybe queued for us before associating to the new AP Added a switch ID in the association response so that the client can tell which APs on the roaming list are on the same switch as the currently associated switch.	Bob Friday
1.18	Modify the loadsharing decision to incorporate the switch ID	Bob Friday

	83894042	
1.19	**Added Tarek's comments on load balancing**	**Bob Friday**
1.20	**Updated the power mgmt section**	**Bob Friday**
1.21	**Updated the loading sharing section with Tarek's minimize handoffs between resiliency domain** **Added Pat's write up on handoffs between mobility groups**	**Bob Friday**

Table of Contents

1 Introduction

This document describes the requirements and design of the client device driver operating in a pico cell environment. The objective of this functional specification / design document is to provide enough detail that the Atheros reference client code can be modified to the support the following requirements:

- Fast roaming in a pico cell environment (2.2 & 2.3)
- Load Sharing and Admission Control (2.3.4)
- WPA Single Authentication Service (2.4)
- Variable Client Receive Sensitivity (2.5)
- Variable Client Transmit Power
- Support Single Data Rate Configuration (2.6)
- Client Power Management (2.7)
- Customized Client API (2.8)
- Support for the new UNII channels (2.9)
- Support for Windows CE platform (2.10)
- Support for non PicoCell networks (2.3)

2 Functional Requirements

2.1 Modifications needed for AeS

To support the custom client driver being developed for SIAC the following modifications / additions are needed to the AeS switch code:

- Information element in the Reassociation Response that contains the roaming candidate list with a switch ID per candidate to be used to minimize switch handoffs.
- Information element in the Probe Response that conveys the AP load in percent of max. allowed associated clients.
- Information element in the Beacon that indicates the AP is part of a pico cell network
- Configuration to enable or disable all this fancy stuff as we want this to be in the mainline code!!
- Implement co channel registers on the AP to allow weak packets to be ignored
- Creation of a list of the APs with the best SNR and switch ID that will be passed to the client as the roaming candidate list
- Configurable SNR threshold for algorithm (Is this advertised in the beacon?)
- Do we need to confirm or update our power save code on the AP?

2.2 Critical Fast Roaming Design Parameters

Table 2-1 shows the critical design parameters used by the fast roaming algorithm.

Design Parameter	Value	Description
Handoff Rate	5 seconds	This is the design goal for handling handoffs under typical walking speeds.
Max Packet Delay	100 msecs	The fast roaming algorithm should not delay packet transmission beyond the value specified here. This value is what effectively limits the amount of time the client can spend scanning potential roaming candidates.
Min. User Throughput	128 kbps	This is the min. half duplex user data rate that must be guaranteed over any 1 second period. This value is what effectively determines the length of the traffic window while looking for a new access point in state 3.
Cell Size	30 ft 5 seconds	This is the smallest cell size the algorithm is designed to handle. At 30' a person walking 6 feet / sec can cross the cell in 5 seconds and if is in the middle of the cell leave it within 2.5 seconds.
Channel Switching Time	4 msecs	This is the maximum amount of time it takes to switch channels. Any packets on the que after 4 msecs will be lost
Directed Probe Request Time	5 msecs	This is the maximum amount of time for a directed probe request / probe response transaction.
Broadcast Probe Request Time	50 msecs	This is the maximum amount of time for a Broadcast Probe request

Table 2-1 Fast Roaming Design Paramters

2.3 Fast Roaming PicoCell Handoff Algorithm

The custom client driver will go into the fast roaming mode when it detects an access point advertising the pico cell information element ID in the beacons. In the fast roaming pico cell mode, the client gets a roaming candidate list in the association response packet when it associates to an access point. The client uses this list of roaming candidates to find another access point when the preemptive handoff threshold is reached. During preemptive handoff decision phase the client alternates between scanning candidates on the roaming list with directed probes and moving traffic to minimize packet latency. In the case that the preemptive handoff fails or the client loses connectivity with the network an active scan of all the available channels is conducted to find an access point.

The fast roaming algorithm will have the following design goals:

1) The fast roaming algorithm can be enabled by the user via the client utility or it will automatically be enabled when the station has located an Access Point which advertises the PicoCelc capability in its beacons and probe responses. Otherwise the standard Atheros roaming algorithm will be used.
2) The fast roaming algorithm will be designed to minimize broadcast probe request traffic
3) The fast roaming algorithm will limit the time that a client is off channel to less than 100 msec out of any 120 msec period of time while the client is associated and has network connectivity
4) The fast roaming algorithm will limit the number of clients that can be connected to a single AP so that the load balancing requirements are met.
5) The fast roaming handoff will be preemptive in nature and roam to another access point before losing connectivity to the associated access point.
6) While in the associated state the client will monitor the SNR of the associated access point at regular intervals. If the client ever loses network connectivity it will scan the list of roaming candidates with directed probe requests (probe requests sent to the broadcast MAC address with specific SSID in the SSID information element) before transitioning to the state of total loss of network connectivity and broadcast SSIDs. When a PCSTA has no connection to an access point, it will perform an active scan using broadcast probe requests to find an access point. A complete passive scan will take (100ms dwell time + 5ms switching overhead) per channel * 20 channels = 2.0 seconds.

Figure 2-1 shows the state diagram of the fast roaming algorithm. State 1 is the desirable stable state of being associated with an access point with a high SNR and monitoring SNR. The goal of the fast roaming algorithm is to be in state 1 and when not in state 1 to get back to state 1 within 300 msec. From state one, one of two things can happen. The first is the loss of network connectivity to the associated access point and the transition to a non associated state where the client will try to re-associate with the access point it just lost connectivity with. The second possibility is a drop in the SNR below the preemptive handoff threshold which will cause the client to transition to the scanning state to select a new access point. If it finds an access point that exceeds the SNR of the existing access point by a specified margin the client will attempt to associate with the new access point. If the client can not find a new access point or fails to associate with the new access point, the client will maintain it's current association and keep looking for a new access point.

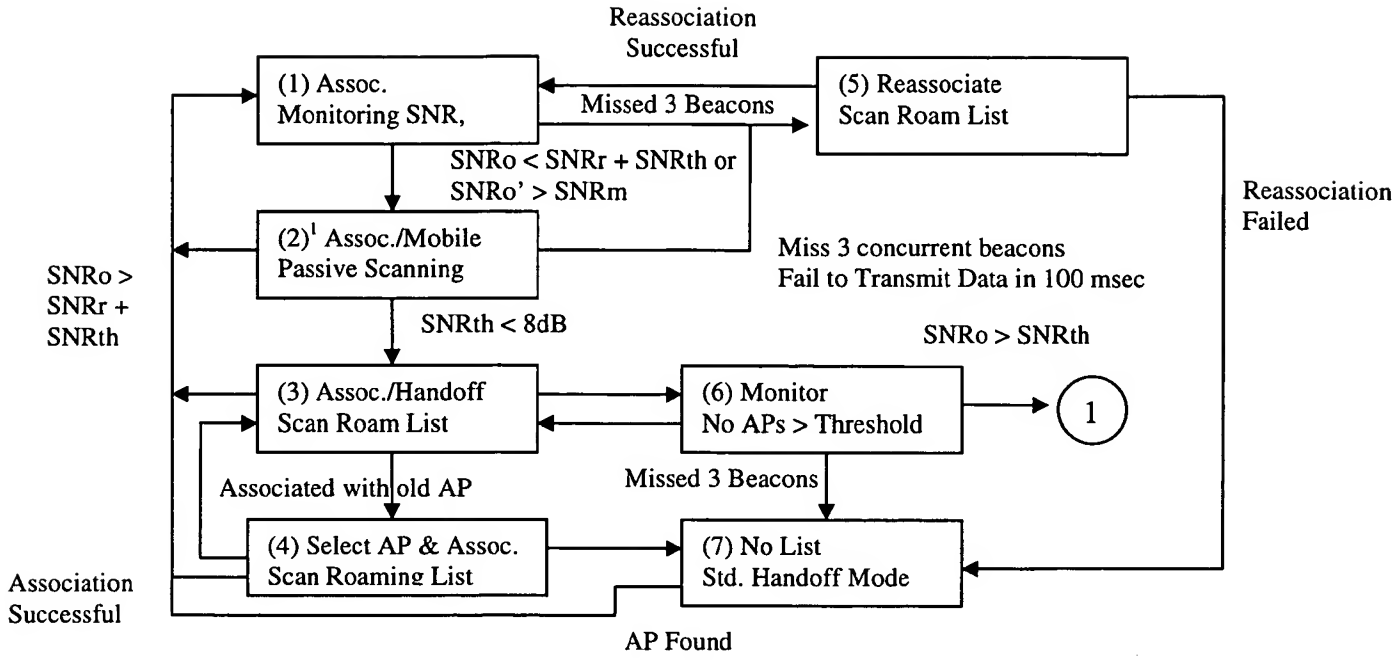


Figure 2-1 Adaptive Scanning State Machine

Notes: 1- State 2 will not be implemented for phase 1 of the project

2.3.1 State 1- Associated with Good SNR

This is the desired state for the client to be in and the goal of the fast roaming algorithm is to keep the client in this state using preemptive handoffs and avoid having to use a full active scan (i.e. state 7) to complete an handoff. In state 1 the client either gets a list of roaming candidates from the APs and creates a filtered SNR sample from a queue of measured SNR samples every 100msecs. The measured SNR samples are taken from beacons and overheard packets from the associated access point. Given a beacon interval of 100msec there should be at least one new measured SNR sample every 100 msecs. Given a filter time constant of 3 samples a sudden change in SNR will be detected in approximately 300 msecs. If the filtered SNR falls below the SNR requirement of the minimum supported data rate plus a configurable margin the AP will initiate a preemptive roaming event and find a new AP to associate with.

2.3.2 State 2- Mobility State

(Note: This state will not be implemented for phase 1 of the project) This state is entered when the change in SNR with respect to time exceeds a threshold indicating that the client is moving or the world around the client is varying significantly. In this state the client will start monitoring the change in SNR (i.e. the first derivative) with respect to time of its roaming candidates in preparation for a handoff.

2.3.3 State 3- Create Roaming List

State 3 is the first step towards a preemptive handoff. In this state, the client sends directed probes to access points in the roaming candidate list to gather the SNR and load information from the access points in preparation for choosing a new access point in State 4. State 3 is made up of alternating scan and traffic windows. During the scan window directed probe requests are sent to each AP in the roaming candidate list for the duration of an AP dwell time. The length of the scan window determines the maximum amount of time the AP will be off channel and thus the maximum packet delay for user traffic. During the traffic window, the client goes back to the channel of its associated access point to move data both up and down. For the SIAC picocell network the default scan and traffic windows will be 50 and 25 msecs respectively. The default state 3 time will be 300 msecs, alternating between scan windows and traffic windows, sending directed probe requests to access points on the roaming list. The maximum amount of time in this state is function of the environment and how fast the SNR changes.

To ensure that we have a good estimate of the SNR to the current AP, the current AP will be sent directed probe requests at the end of scanning the roaming list. The current AP will always be the last AP probed to get the most up to date picture of the current SNR value. The average SNR of the current AP will now be used as the point of reference during the selection process rather than the SNR filter output. In the event that the current AP does not respond to any probe requests, the client will assume that the AP is out of range and will use an SNR average of 0 as the comparison value. To be considered, a candidate AP must have a SNR average above the current AP's SNR average by the specified margin (i.e. default is 6dB). If the current AP does not respond and no candidate AP is valid (none responded to probes), the client will transition to the connection lost state (7) and start the disconnect timer.

There are two timers used in this state. The first is an interrupt driven NDIS driver and the second is a polled hardware timer. The probe request timeout uses the interrupt driven NDIS timer provided by the windows OS. This timer has a typical limited accuracy of -0/+6 msecs. Thus a 3 msec probe request timeout may take 3 to 10 msecs. The dwell time per access point is driven by polling an NDIS hardware timer provided by the Windows OS. The dwell time limits the maximum number of probe requests that will be sent by the client. A typical probe request / probe response transaction takes 0.5 to 1 msec under no load conditions. The hardware timer is accurate to within 100's of usecs. To ensure that a minimum number of probe requests are tried per AP, a mechanism is provided to make sure a minimum number of probe requests are tried per AP.

. Given an RF redundancy factor of 3 to 6, 3 to 6 access points on the list with a very high SNR are most likely covering the same area as the associated access point and are not likely roaming candidates. (Note: Having more than one AP to cover the same area is needed for failure scenarios and to satisfy peak capacity requirements.) The goal is for a roaming candidate to be on the list 99% of the time under all conditions. Given a channel switching time of 4 msecs and a Directed Probe Request / Probe Response transaction time of 2 msecs under no load conditions the SNR of an access point can be characterized in 10 msecs or less with 3 probe requests. Given a maximum off channel time of 100 msecs, 6 access points can be typically characterized in 100 msecs. At the end of 100msecs or completion of scanning the entire roaming list the client will enter the association state and attempt to associate with a new access point. In response to the directed probe request the access point sends the following information in the probe response:

2.3.4 State 4- Associate with a AP and Load Balancing

In this state the client attempts to roam to a new AP based on the SNR and load factor obtained in State 3 from the probe responses and the switch ID obtained in state 1 from the roaming candidate list. The selection process for the new AP works by first ranking the candidate APs by SNR. The SNR ranking is from best (largest SNR) to worst. All roaming candidates that have an SNR better than the current AP's SNR (or 25dB if the current AP's SNR is greater than 25) by the specified margin are kept to form a new association list . This new list is then broken into 6 groups:

1. Group 1- APs with a load factor < AP load threshhold and a switch ID equal to that of the current AP
2. Group 2- APs with a load factor < AP load threshold, a switch ID and resiliency ID equal to that of the current AP
3. Group 3- APs with a load factor < AP load threshold and a switch and resiliency ID does NOT equal to that of the current AP
4. Group 4- APs with a load factor > AP load threshold and a switch ID equal to that of the current AP
5. Group 5- APs with a load factor < AP load threshold, a switch ID and resiliency ID equal to that of the current AP
6. Group 6- APs with a load factor > AP load threshold and a switch and resiliency ID NOT equal to that of the current AP

Within each group the APs are ranked by SNR. The client will then try to associate with an AP starting with group 1 and moving to group 6. The AP load threshold is a utilization factor that indicates what percentage of the APs capacity in terms of associated clients is being utilized. For example, given an AP's maximum capacity is 12 clients it will advertise 50% utilization when there are 6 clients associated. The default maximum capacity of an AP is 12 and the default AP load threshold is 75%. If the re-association fails, the client will move to the next best AP in the list and attempt to re-associate. If the candidate list is exhausted with no successful re-association, the client will re-associate to the original AP and return to state 3 to re-scan the candidate list. If no candidate meets the minimum SNR and loading requirements, the client will maintain its association with the current AP and return to state 3 to re-scan the candidate list.

2.3.5 State 5- Reassociate

State 5 indicates that the client has stop hearing beacons from it's associated access point. There are a couple of reasons for going from state1 to state 5:

- The AP has failed
- The client has moved out of coverage very quickly

When the client finds itself in this state it will immediately try to reassociate with the original access point. If it fails to reassociate it will attempt to find another access point on the roaming candidate list before going to state 7.

2.3.6 State 6- Monitor State

The backoff state will be entered when the client has completely scanned the entire candidate list 'n' consecutive times with no candidate AP being better than the current AP. The initial implementation shall use 3 for the value of n. While in the backoff state, the client will continue to monitor the current AP's SNR by running the sampled SNR of beacons through the SNR filter. If the SNR filter output rises above the threshold plus the margin value, the client will return to the monitor state (1). If the client misses 'm' number of missed beacons, the client will start an active broadcast scan and transition to the connection lost state (7), starting the disconnect timer as described above. The value used for m will be the same as that used in the monitor state (1). When the backoff state is entered, a backoff timer will be started. The backoff timer will be set with a value of 500ms plus a random number of additional milliseconds between 0-500. If the client has not lost media connection and has not transitioned back to the monitor state when the backoff timer expires, the client shall transition to the candidate search state (3) again and re-scan the candidate list like normal

2.3.7 State 7- Network Connection Loss

State 7 is entered during initial power up and when the preemptive handoff mechanism fails. In this state the client will actively scan all channels looking for an access point. If the client can not find an access point within a specified time (i.e. default = 10 seconds) a disconnect timer will be used internally to notify the OS of the loss in media connection. Any data being queued from the OS network stack when in this state will only be queued until the driver's TX data queues become full, at which point any new data received will be dropped by the driver. The disconnect timer will default to the same value used by the normal Atheros driver: 10 seconds. When the timer expires, the OS will be notified of the loss in media connection and the pico-cell state machine will stay in the connection lost state (7).

2.3.8 Mobility Group Handoff

All switches within a mobility domain will advertise their Mobility Domain IDs (MDID) in both the probe response and beacon packets. The format of the MDID will be the Airespace OUI followed by the configured mobility domain Identifier (which is separate from the mobility domain name).

The MDID is used by the client to determine whether a previously created PMK (and potentially the associated PTK) may be re-used. When a station encounters an access point that is advertising a new MDID, it recognizes that an 802.1X authentication will be required (or it must have a cached PMK/PTK that was previously created via a successful authentication). In order to be capable of caching PMK/PTKs for various mobility domains, it will be required for the station to include the MDID in its key cache entry.

When a station associates with an AP in a new mobility domain, it MUST include the IP address of the switch it was previously associated with. This also require that the association response sent include the IP address of the switch in the 'Previous-Switch-Address' IE, which must be stored by the station's driver. When a switch receives an association request with a 'Previous-Switch-Address' IE. Once the association is complete, the new switch must send a inter-domain mobility notification (IDMN) to the switch specified in the Information Element. The message will be sent by the mobility manager, and will be secured using a 'inter-mobility domain secret'. Furthermore, the mobility manager will recognize that when this message is issued, there is no need to issue an announce message.

The sending switch will also recognize that it must determine whether credentials are already present, or whether a full 802.1x authentication exchange will be required. The switch will also allow the DHCP phase to complete, but it MUST NOT plumb the rule or respond to ARPs during this time (nor should it send the XID or gratuitous ARP until it has received a response from the previous switch).

Upon receipt of this message, the previous switch will immediately remove the rule from its NPU and delete its ARP entry for the station.

There exists a potential race condition that could occur if a station device were to ping/pong across two switches within different mobility domains. In order to eliminate the potential for a station to return and associate with an AP in the previous mobility domain before the IDMN message is received, the station will make use of a hand-off count, which is included in the IDMN message. The client increases its hand-off count in every handoffs, and include it in the 'Handoff-Counter' IE in the Association Request messages. Switches make use of the Handoff Counter' IE to detect ping pong events, by evaluating whether the counter in the Association Request is greater than the value found in the IDMN message. For instance, if the association request contains a counter that is higher than the IDMN message, it will acknowledge the message, and initiate its own IDMN message (because the station is coming back).

All Probe Responses and beacons sent by an AP will include the Mobility Domain ID (MMID). A station must cache the MMID of the last AP it had associated with.

Stations must maintain a handoff counter, which is monotonically incremented everytime a station issues an Association Request to a new AP (meaning the message is sent to an AP other than the one the station is currently association with). The counter is included by the station in the Handoff-Counter IE.

When a station transmits an Association Request to an AP that is advertising a Mobility Domain that differs from the one that was advertised by the AP the station was previously advertised with, it must include the Previous-Switch-Address Information Element, which the station received in the previous Association Response.

When the switch receives an Association Request with a Mobility Domain ID that differs from its current mobility domain, it must invoke the mobility manager to request that a inter-domain mobility notification be sent to the IP address found in the Previous-Switch-Address IE.

The AP must include the Previous-Switch-Address IE, which includes its switch's IP address.

2.3.8.1 Switch Failure

The way the infrastructure is configured in the SIAC system, each AP's switch association could change (due to a failure) during normal operation. The net result is that the switch ID and MGID, if provided during the client's (re)association, may not be accurate when the client starts the roaming process. To better manage this information, the client driver will update the switch ID and MGID for every candidate during the candidate search state (3) based on the information the AP is providing the probe response and beacon frames. This is in addition to the loading information and average SNR that are also gathered at this time.

2.3.9 SNR Filter

For each beacon overheard from an access point, an SNR sample is obtained. These SNR samples are feed into a recursive filter and the output of the filter used to make state transition decisions and AP selection decisions. To make mobility decisions at a rate of a handoff every 5 seconds the SNR information needs to be sufficient to get a filter output every 100 msecs. Given a beacon interval of 100msec there should be at least 1 SNR sample available every 100 msecs. The filter coefficients need to be selected to allow the filter output to settle with in 1 second or 10 samples.

SNRout = $\beta 1$ * SNRold + $\alpha 0$ * SNRnew

$\beta 1 = x$

$\alpha 0 = 1-x$

The value for x can be directly specified, or found from the desired *time constant* of the filter. Just as $R \times C$ is the number of seconds it takes an RC circuit to decay to 36.8% of its final value, d is the number of samples it takes for a recursive filter to decay to this same level:

$$x = e^{(-1/d)}$$

Time constant of single pole filters. This equation relates the amount of decay between samples, x, with the filter's time constant, d, the number of samples for the filter to decay to 36.8%.

For instance, a sample-to-sample decay of corresponds to a time x ' 0.86 constant of samples. There is also a fixed d ' 6.63 relationship between x and the -3dB *cutoff frequency*, , of the digital filter: fC This provides three ways to find the "a" and "b" coefficients, starting with the time constant, the cutoff frequency, or just directly picking x.

$$x = e^{(-2 * \pi * f}$$

2.3.10 SNR Characterization Data

SNR Filter Performance in a PicoCell

3-25-04 (Data Collected 3-22-04 to 3-23-04)

Test Description:

The purpose of this test was to determine the behavior\profile of client SNR in terms of reliability and repeatability under conditions of client movements in a single picocell. This test required the use of a custom client utility to measure and log associated SSID beacon packets.

Test Configuration

All data was collected with the following conditions:

- Client data was collected at a height of 4' at all times.
- AP Antenna height was at 8' at all times with approximate 45 degree down-tilt.
- 5GHz 802.11a
- Airespace AP1200 A/B
- AP Transmit Power Level of 4 (~0dBm)
- Antenna Peak Gain of 5dBi (Tower Six)
- AP Diversity Enabled
- Client DLINK AirExpert DWL-AG650 (Atheros 5212)
- Client Diversity Enabled
- Client Laptop IBM Thinkpad T41
- Intelligraphics Modified Driver

Data Analysis

All Data consisted of beacons only, collected at a rate of 100mSec periodic rate.

Standard IIR Filter characteristics were set at Alpha = 0.75 and Beta = 0.25.

Data Collected:

1. Stationary @ 6' (non-shadowed)
2. Stationary @ 10' (shadowed)
3. Spinning in place @ 6' (non-shadowed)
4. Moving behind a shadow 10' from Antenna
5. Moving around a corner 10' from Antenna (shadowed)
6. Moving under and behind the antenna (non-shadowed)
7. Walking 80 feet across the face of the antenna
8. Running 80 feet across the face of the antenna

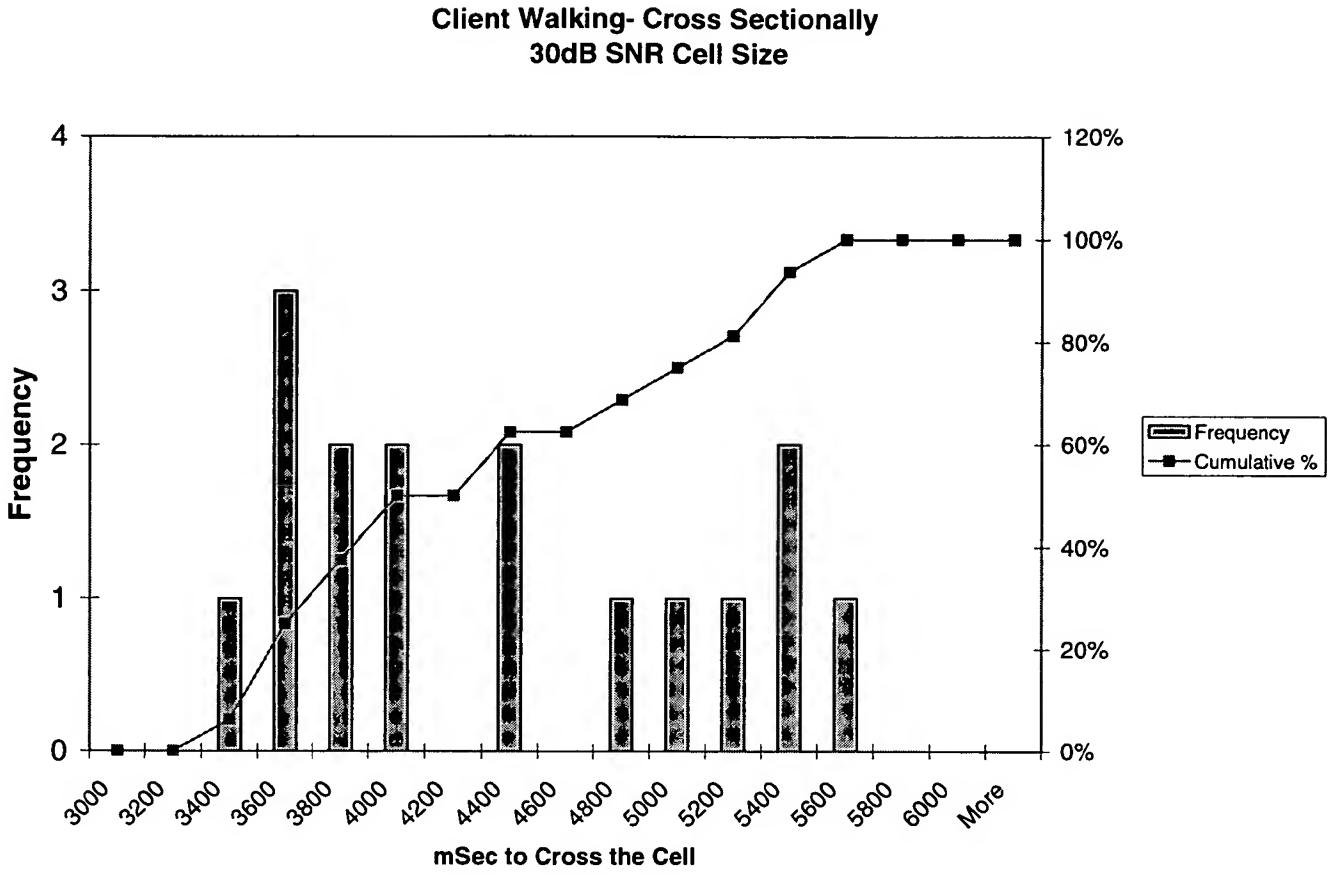
Conclusion:

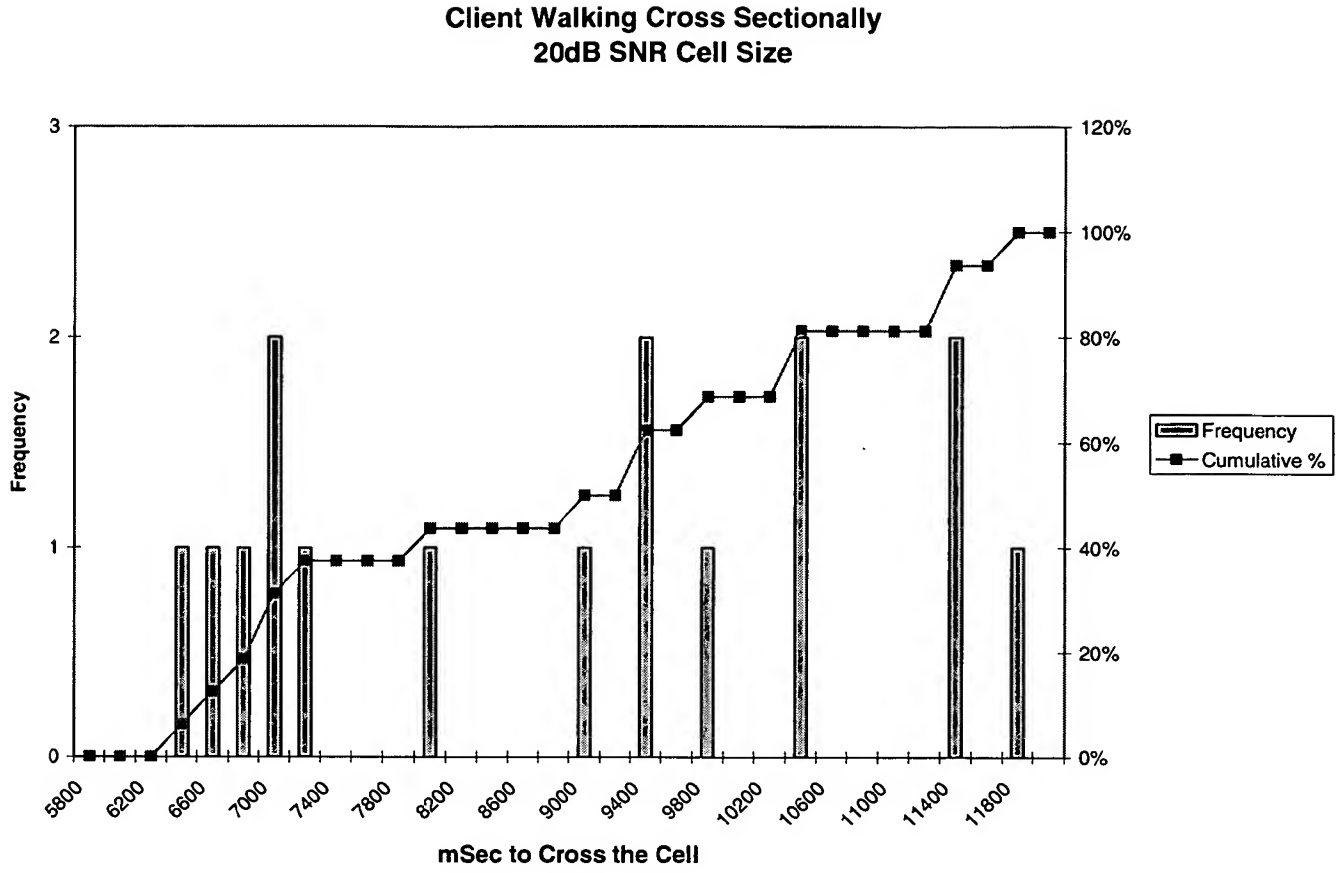
Data was collected for stationary positions and several movements around a single AP antenna to determine the effects on client SNR. All data was processed based on an IIR filter coefficient of Alpha=0.75 and Beta=0.25. This empirically was a good compromise between response, delay, and smoothing resulting in an approximately 300mS delay. Analysis of all motions resulting in a SNR drop below 20dB resulted in a histogram to determine how fast it occurred. Upon exiting a picocell, typical time to drop from 30dB to 20dB walking out of a picocell is about 2 seconds, running is about 1 second. Due to the typical effects of motion\walking on SNR, in order to not exceed 50(80)% of beacon packets below 17dB SNR, the appropriate threshold to roam is approximately 23(25)dB.

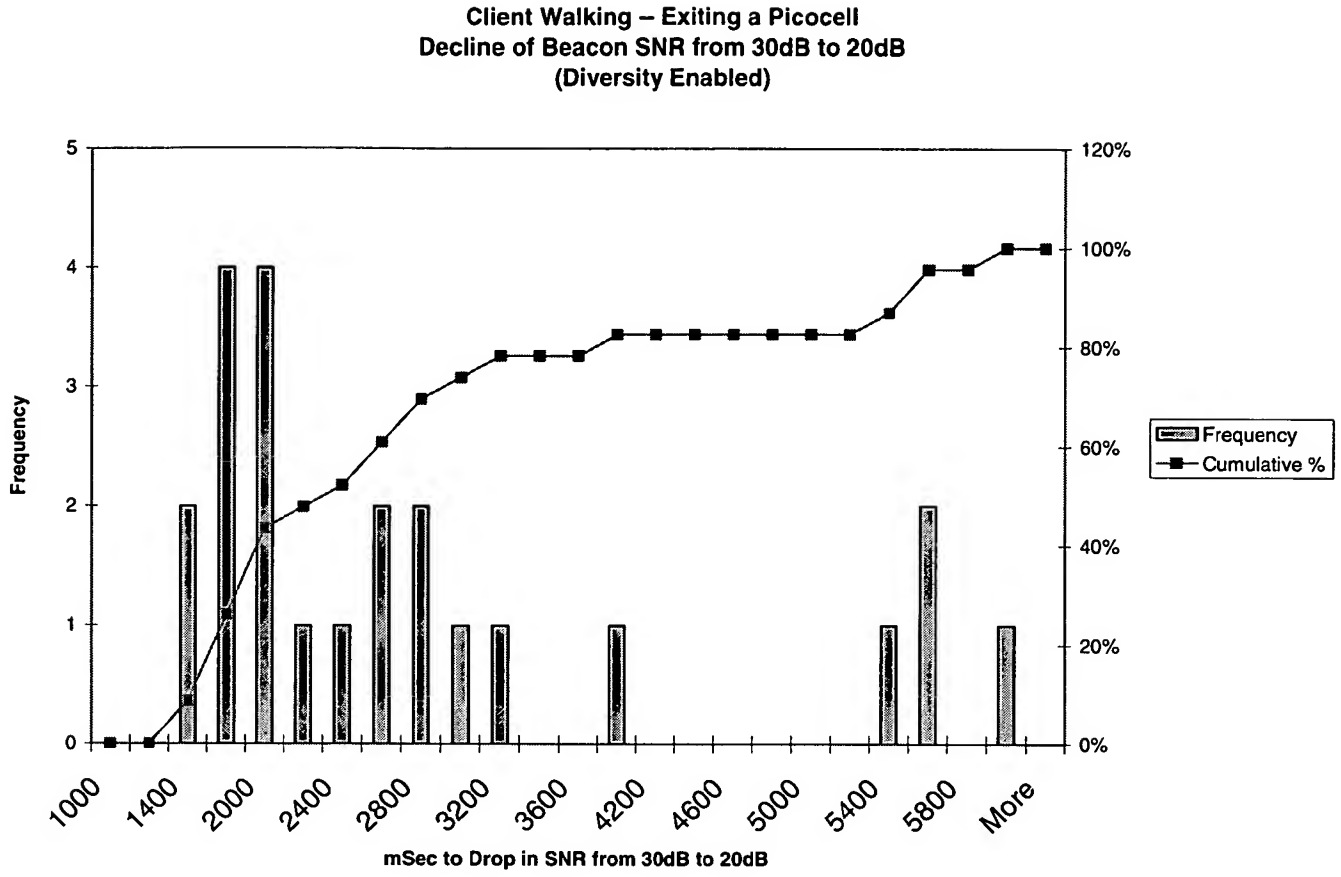
Notes: During this experiment it was discovered that every 60 seconds, for some data sets, beacons were coming out at full transmit power. If the transmit power effected any data analysis (i.e. Histograms) the data for that time frame was thrown out, as it was generally causing outliers.

Results:

	Min (mSec)	Max (mSec)
Client Walking (30-20dB drop)	1400	6000
Client Running (30-20dB drop)	700	2000
Cell Size (20dB SNR)	6400	11800
Cell Size (30dB SNR)	3400	5600


Client Walking- Cross Sectionally
30dB SNR Cell Size
Frequency
mSec to Cross the Cell
0
1
2
3
4
0%
20%
40%
60%
80%
100%
120%
3000
3200
3400
3600
3800
4000
4200
4400
4600
4800
5000
5200
5400
5600
5800
6000
More
Frequency
Cumulative %


Client Walking Cross Sectionally
20dB SNR Cell Size
Frequency
mSec to Cross the Cell
Frequency
Cumulative %
0
1
2
3
0%
20%
40%
60%
80%
100%
120%
5800
6200
6600
7000
7400
7800
8200
8600
9000
9400
9800
10200
10600
11000
11400
11800



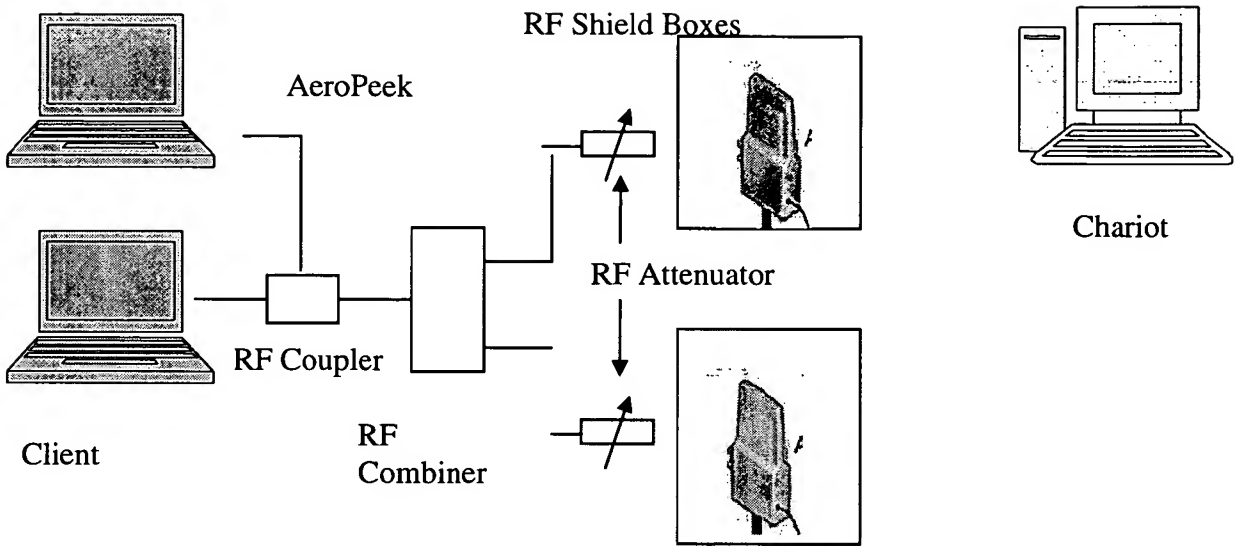
2.3.11 Handoff Requirements and Test Procedure

This section describes the handoff specification and the test procedure to measure handoff / mobility performance.

Pico Cell Handoff Requirements		
Spec	Value	Comments
Handoff Rate	5 secs	This specification is based on a person walking around a post at normal walking speeds.
Handoff Time	100msec	Handoff time is defined as the maximum time that client can not send a packet to a access point.

Table 2-2 Handoff Specifications

2.3.11.1 Shield Box Test Procedure



2.3.12 Channel Switching Time

While the actual time to switch channels is short (i.e. < 1msec), the time to reset the baseband chip and to allow ques to empty can take several 1 msecs. This section looks at details of switching channels and methods of speeding up the channel switching time. The channel switching time can optimized by making the time limit on how long to wait for the ques to empty a function the minimum supported data rate.

2.3.13 Interpretation of Status Codes and Reason Codes

The client shall interpret all Status and Reason Codes sent in 802.11 MAC Management frames. For any unsuccessful, i.e., nonzero, code, the client shall perform the following actions.

Value	Description	Action
0	Successful	None
1	Unspecified failure	Try association at another AP. Do not attempt to associate with the same AP that returned this code.
2-9	Reserved	None
10	Cannot support all requested capabilities in the Capability Information field	Correct Capability Information Field and retry association
11	Reassociation denied due to inability to confirm that association exists	Use Association Request, instead of Reassociation Request

Value	Description	Action
12	Association denied due to reason outside the scope of this standard	TBD
13	Responding station does not support the specified authentication algorithm	Use correct authentication algorithm and retry authentication. Do not attempt another authentication until the authentication algorithm has been changed.
14	Received an Authentication frame with authentication transaction sequence number out of expected sequence	Correct sequence numbering and retry authentication
15	Authentication rejected because of challenge failure	Do not attempt another authentication until the underlying reason for failure has been corrected. This is likely due to a mismatch of shared secret or WEP keys.
16	Authentication rejected due to timeout waiting for next frame in sequence	Retry authentication.
17	Association denied because AP is unable to handle additional associated stations	Try association at another AP. Do not attempt to associate with the same AP that returned this code.
18	Association denied due to requesting station not supporting all of the data rates in the BSSBasicRateSet parameter	Correct the rates in the basic rate set and retry association. Basic rates must match those of the AP.
19	Association denied due to requesting station not supporting the Short Preamble option	Remove Short Preamble from CIF, disable its use in the station, and retry association.
20	Association denied due to requesting station not supporting the PBCC Modulation option	Remove PBCC from CIF, disable its use in the station, and retry association.
21	Association denied due to requesting station not supporting the Channel Agility option	Enable support for channel agility, set the bit in CIF, and retry association.

Table 2-3, Required Actions for Individual Status Codes

Value	Description	Action
0	Reserved	
1	Unspecified reason	Find a new AP to reassociate or authenticate with.
2	Previous authentication no longer valid	Begin with initial Authentication frame (sequence number 1)
3	Deauthenticated because sending station is leaving (or has left) IBSS or ESS	Find a new AP to reassociate or authenticate with.
4	Disassociated due to inactivity	Reassociate with this or another AP.
5	Disassociated because AP is unable to handle all	Find a new AP. Do not reassociate

Value	Description	Action
	currently associated stations	with AP that sent this code.
6	Class 2 frame received from nonauthenticated station	Authenticate with AP
7	Class 3 frame received from nonassociated station	Associate/reassociate with AP before sending data frames.
8	Disassociated because sending station is leaving (or has left) BSS	Find a new AP. Do not reassociate with AP that sent this code.
9	Station requesting (re)association is not authenticated with responding station	Authenticate with AP first.

2.4 WPA Single Authentication Service

The client shall support the single authentication service for 802.1X-based authentication mechanisms.

The client shall always use the 802.11i PMK caching mechanism. After an initial EAP authentication that generates a PMK, the client shall always present the PMKID of the most recently created PMK associated with the SSID to which the client is associating in the reassociation request. Upon successful reassociation, the client shall proceed to the EAPOL-key exchange, as described in 802.11i/D8.

2.5 Variable Client Receive Sensitivity

In a Pico Cell environment we would like to configure the access point to ignore packets with a low signal strength so that access points that are sharing the same channel are not constantly waiting to transmit because they are hearing weak signals from other radios. The receiver sensitivity of a typical access point is -90 dBm or better. Typically in a pico cell environment the signal strength between the clients and the associated access points is relatively high (e.g. > -65 dBm). Given an SNR requirement of 15 dB you would like to tell the access point to only defer transmission is you hear 802.11 traffic at signal strength levels greater than -80 dBm (i.e. -65 dBm - 15 dB). The following sections describe different mechanisms that can be used to limit the effective receiver sensitivity for the Atheros chipset.

2.5.1 Compatible Chipsets

This table shows for which chipsets the co channel registers are supported.

	Nortel Client 2201 AR5211/5111/2111	Airespace AP AR5212/5111/2111	Client X AR5212/5112	Nortel Client 2202 AR5213/5112	New Airespace AP (Dlink\Wistron) AR5312/5112/2112
Ignore \ Reception Start					
Cyclic Preamble Threshold	-	X	X (assume)	X (assume)	X (assume)
Signal Jump Threshold	-	X	X (assume)	X (assume)	X (assume)
CCA Signal Threshold	-	X	X (assume)	X (assume)	X (assume)
Reception Restart					
Restart Enable	-	X	X (assume)	X (assume)	X (assume)
Large Signal Jump Threshold	-	X	X (assume)	X (assume)	X (assume)
Reception Drop					
Abort on Power Drop Enable	-	X	X (assume)	X (assume)	X (assume)
Raw Power Drop Threshold	-	X	X (assume)	X (assume)	X (assume)
Abort Low RSSI Threshold	-	-	-	X (assume)	X (assume)
Low RSSI Threshold	-	-	-	X (assume)	X (assume)
Abort Wrong BSSID Enable	-	-	-	X (assume)	X (assume)
Abort Wrong BSSID Data Only Enable	-	-	-	X (assume)	X (assume)
Transmit					

Stomp					
Stomp Low RSSI Enable	-	X	X (assume)	X (assume)	X (assume)
Low RSSI Threshold	-	X	X (assume)	X (assume)	X (assume)
Stomp Wrong BSSID Enable	-	X	X (assume)	X (assume)	X (assume)
Stomp Wrong BSSID Data Only Enable	-	X	X (assume)	X (assume)	X (assume)

2.5.2 Co Channel Interference Modifications

The base driver code (3.1.1.12) auto-adjusts the cyclic power threshold value under certain conditions (like when scanning).

2.5.3 Ignore

The ignore feature consists of 3 parameters that can be adjusted to make the receiver deaf to weak signals. The three knobs are:

Parameter	Default	Description
bb_cycpwr_thr1		This parameter sets the RSSI threshold that specifies the SNR at which packet reception starts. The client will not start packet reception if the power level is above
bb_rssi_thr1a		This parameter specifies the jump in SNR at which to trigger start of reception.
bb_thresh62	**-62dBm**	This parameter specifies the threshold at which a transmitter will defer. If a client detects energy above level it assumes the channel is unavailable and defers transmission.

2.5.4 Restart

Restart can be enabled to allow the receiver to restart reception in there is a sudden jump upward in the receive power level.

Regisiter	Default	Description
bb_enable_restart		Enables the restart feature
bb_restart_lgfirpwr_delta		Sets the threshold of how much a jump (in dB) is required to trigger restarting looking for a new packet

2.5.5 Drop

Drop allows the reception of a packet to be terminated, and the search for a new packet began. This is triggered based on a sudden drop in received power,

Parameter	Default	Description
bb_enable_pwr_drop_err		Enables the feature of dropping a packet when there is drop in raw power
bb_pwrdrop_lgfirpwr_delta		Sets the threshold of how much change there must be in a packet before it is dropped
Mc_xr_rx_abort_rssi		Enables aborting on low RSSI
Mc_xr_rx_abort_rssi_thresh		Set the threshold in RSSI at which a packet will be dropped.
Mc _xr_rx_abort_rx_abort_bssid		Enables aborting on wrong BSSID
mc_rx_abort_data		Causes only data frames from wrong BSSID to be aborted (mgmt and control frames are still received)

2.5.6 Stomp

Stomp parameters control whether the transmitter is allowed to transmit over an active reception. This can based on wrong BSSID or received RSSI.

(Note: Stomp requires Restart)

Regisiter	Default	Description
mc_xr_tx_stomp_rssi		This enables stomping on low RSSI packets
mc_xr_tx_stomp_rssi_thresh		Sets RSSI value on which stomp occurs

mc_xr_tx_stomp_bssid		Enables stomping of packets from wrong BSSID
mc_xr_tx_stomp_data		Causes only data packets (not management or control frames) to be stomped on the basis of BSSID)

2.5.7 Implementation Details

Note: PCU reset occur on both cold and warm resets: both cold and warm reset will cause the pcu registers to go to their reset state as described below.

0-1FF PCU:

Address Name Bits Reset Description
(Int Addr: 000)

Note: while the file with baseband registers is built off a register offset of 0x600, The MAC register related to stomp and restart is shown as an absolute value in hex.

##########

80D0 Extended Range Stomp
(Int Addr: 034, Access: R/W, Clock: system clk)

XRSTMP	15:0	0	bit 0:	XR_RX_ABORT_RSSI
		0	bit 1:	XR_RX_ABORT_BSSID
		0	bit 2:	XR_TX_STOMP_RSSI
		0	bit 3:	XR_TX_STOMP_BSSID
		0	bit 4:	XR_TX_STOMP_DATA
		0	bit 5:	XR_RX_ABORT_DATA
		'h25	bit 15:8:	XR_TX_STOMP_RSSI_THRESH
		'h25	bit 23:16	XR_RX_ABORT_RSSI_THRESH

Extended Range Description:

XR_TX_STOMP_RSSI enables the transmit stomping of receive packets with a low RSSI. See description of XR_TX_STOMP_RSSI_THRESH.

0: disable xr_tx_stomp_rssi mode
1: enable xr_tx_stomp_rssi mode

XR_TX_STOMP_BSSID enables the transmit stomping of receive packets which do not match our BSSID. Frames directed to this STA will not be transmit stomped.

0: disable xr_tx_stomp_bssid mode
1: enable xr_tx_stomp_bssid mode

XR_TX_STOMP_DATA enables the transmit stomping of receive packets which are of type data.

0: disable xr_tx_stomp_data mode
1: enable xr_tx_stomp_data mode

All the transmit stomp modes which are enabled will need to pass the corresponding critera for the transmit stomp to occur. Let's take the situation where XR_TX_STOMP_RSSI and XR_TX_STOMP_BSSID are both set.

Then both the low RSSI and non matching BSSID conditions must occur for transmit stomp to happen. Transmit stomp uses the pcu_channel_idle to trick the DCU into thinking that the channel is clear.

XR_RX_ABORT_RSSI enables the receive abort of receive packets with a low RSSI. See description of XR_RX_ABORT_RSSI_THRESH.

0: disable xr_rx_abort_rssi mode
1: enable xr_rx_abort_rssi mode

XR_RX_ABORT_BSSID enables the receive abort of receive packets which do not match our BSSID. Frames directed to this STA will not be receive aborted.

0: disable xr_rx_abort_bssid mode
1: enable xr_rx_abort_bssid mode

XR_RX_ABORT_DATA enables the receive abort of receive packets which are of type data.

0: disable xr_rx_abort_data mode
1: enable xr_rx_abort_data mode

All the receive abort modes which are enabled will need to pass the corresponding critera for the receive abort to occur. Let's take the situation where XR_RX_ABORT_RSSI and XR_RX_ABORT_BSSID are both set. Then both the low RSSI and non matching BSSID conditions must occur for receive abort to happen. Receive abort uses the rx_abort signal to notify the baseband to stop receiving this frame and start searching for a new frame.

XR_TX_STOMP_RSSI_THRESH is the threshold for the receive signal strength indicator for use by transmit stomp on receive. If the RSSI

from the first byte of the receive frame from the baseband is less
than this value, then the packet is a candidate to be transmit stomped.

XR_RX_ABORT_RSSI_THRESH is the threshold for the receive signal strength
indicator for use by receive abort on receive. If the RSSI
from the first byte of the receive frame from the baseband is less
than this value, then the packet is a candidate to be receive aborted.

PHY registers associated with stomp and restart for mitigating co-channel interference.

```
#
# This file is relevant to the AR5213.  It may not be correct for other
# chips.
#
# --------------------------------------------------------------------------
#
# The pin format shall have the following fields, all contained in a single
# line separated by white space(s).  For easy parsing, field values shall
# not have any spaces, except for the comment.  A white space
# is either a space or tab.
#
#    Required:
#
#      name          := signal/bus name.  Busses will be of the form bus[msb:lsb]
#      type          := r, rw (read or read/write; no write only)
#      numbits       := number of bits in register
#      reset value   := value of register upon cold and warm reset
#      address       := address on configuration interface

#
################################################################
# NOTE: all register addresses below have an offset of 0x600
# The register numbers shown below are in decimal, and represent (in decimal) the offset from 0x600.
################################################################
#
# name              type   #bits/ cold    warm    [comment]
#                            default reset   reset
# ====              ====   ==    =====   =====   =========


# reg 25: cca
minCCApwr           rw     9'h000          # [27:19] read: measured minCCApwr write: NA          xz
                                           #  signed, in dB step
thresh62            rw     7'h1a                 # [18:12] dB above noisefloor required for CCA
```

```
cca_count_maxC      rw   3'h3        # [11:09] Max # of loops (512) per noisecal
maxCCApwr           rw   9'-180      # [08:00] Initial/forced value of noisefloor
                                     #      signed, in half dB step

                                     # reg 73: Timing control 5

    long_sc_thresh_hi_rssi rw  7'd32     # [29:23] threshold for self-corr of longs (hi rssi)  yw
    rssi_thr1a             rw  7'1       # [22:16] threshold thr1a for rssi (unsigned in dB)   xz
    enable_rssi_thr1a      rw  1'b1      # [15:15] enable to gate agc_done with                xz
                                         #      rssi > rssi_thr1a for strong signal
    cycpwr_thr3            rw  7'10      # [14:8] cyclic power threshold3                      xz
                                         #      (unsigned, in dB)
    cycpwr_thr1            rw  7'0       # [7:1]  cyclic power threshold1                      xz
                                         #      (unsigned, in dB)
    enable_cycpwr_thr1     rw   1'b1     # [0]  enable to gate m1flag with                     xz

    cycpwr > cycpwr_thr1

                                         # reg 92: restart xz


weak_rssi_vote_thr          rw   7'100   # [28:22] use voting if rssi is larger than
weak_rssi_vote_thr
                                         #  for weak signal detection to decide whether it
                                         #  is an ofdm or cck packet
enable_ant_fast_div_m2flag rw    1'b1    # [21:21] enable fast antenna diversity for ofdm weak
                                         # signal detection (m2flag)
ant_fast_div_gc_limit       rw   3'2     # [20:18] Allow fast antenna diversity if the number of
                                         #  consecutive gain changes is less than this value
ofdm_cck_rssi_bias          rw   6'-5    # [17:12] ofdm cyclic rssi bias for 11g to decide
                                         # whether it is an ofdm packet or cck packet
                                         # signed, in dB step
pwrdrop_lgfirpwr_delta      rw   5'd10   # [11:7] threshold for power drop, unsigned, in dB step
enable_pwr_drop_err         rw   1'b0    # [6:6]  enable to check power drop for ofdm packet
restart_lgfirpwr_delta      rw   5'd10   # [5:1]  threshold for restart, unsigned, in dB step
enable_restart              rw   1'b0    # [0:0]  enable strong signal restart
```

2.6 Multirate Operation

The client shall interpret and act upon the data rates sent in the Supported Rates information element included in Probe Response, Beacon, Association Response, and Reassociation Response frames. The client shall transmit frames using only the data rates that are contained in the Supported Rates information element. For the NYSE the supported data rate is 36 Mbps.

2.7 Power Management

The objective of the power management requirement is to enable significantly increased standby times for WLAN client devices.

The client should be in its power conservation state as much as possible for the applications supported by the client. The AP will buffer all frames for a client that is in the power conservation state for at least the amount of time indicated by the Listen Interval field of the most recent Associate Request or Reassociation Request from the client. The AP will begin to discard frames that have been buffered for longer than the Listen Interval by a specified aging interval. When one or more frames are buffered for a client, the AP will indicate the buffered frames by setting the bit in the TIM that corresponds to the Association ID assigned to the client. The AP will also indicate that additional frames are buffered for a client that is in the power conservation state by setting the More Data bit in each Data frame sent to the client.

The switch will also perform proxy ARP for all clients associated with APs connected to the switch. This enables a client to determine its sleep durations based on application requirements and not DTIM intervals, if the client does not require receipt of other multicast frames. In this power conservation state, the client will not wake for DTIM transmissions. Thus, it will not receive any broadcast transmissions that are buffered by the AP and transmitted at DTIM intervals.

2.7.1 SIAC PDA Usage Profile

2.7.2 Nortel 2201 Mobile Adapter Power Consumption

Nortel Networks WLAN - Mobile Adapter 2201 uses an operating voltage of 3.3 VDC, +/- 5%. The WLAN card has two power aspects: one associated to the card DC power consumption (how much energy it needs to run, how long your laptop battery will last...) and the one associated with the radio power (how strong/far/good the radio is...) both in transmission and in reception. Both power aspects are tightly linked (if you transmit more on 5GHz you will consume more power than on 2.4GHz).

You have the following configurations for the power consumption: power saving mode off1[1], normal and maximum. Indeed the power management functions by putting the radio to sleep (i.e. lowering the power drain) when no transmission activity occurs for some specific time period. Here are the 2201 **power consumptions** for different states:

1) Transmit Mode : 350mA @ 3.3V (1155 mW)
2) Receive mode: 370mA @ 3.3V (1221 mW)
3) Standby mode: 97mA @ 3.3V (297 mW)
4) Power save mode: 12mA @ 3.3V (39.6 mW)

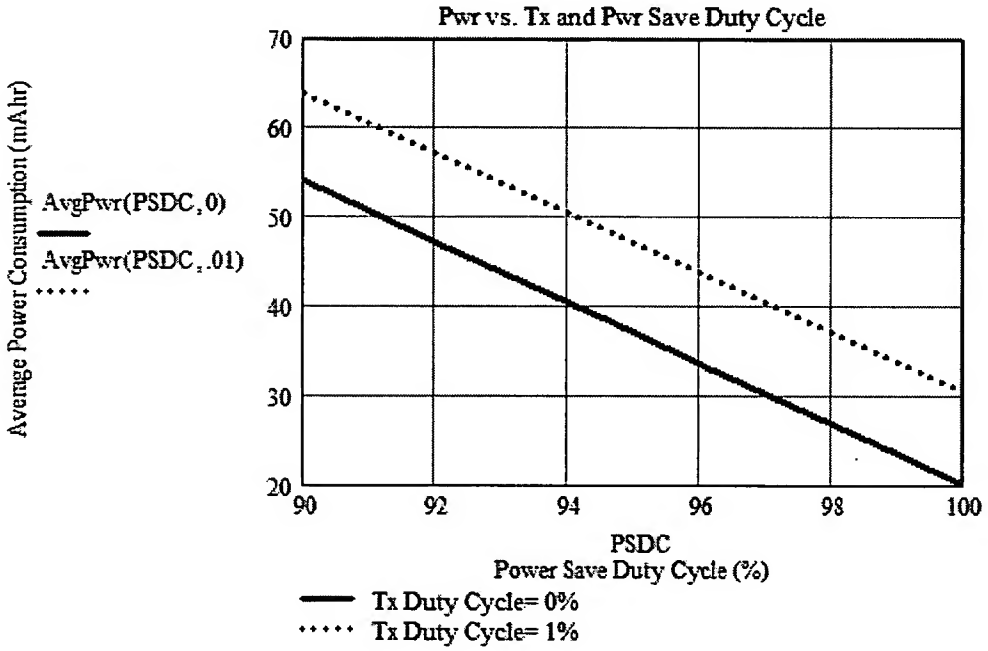
2.7.3 Nortel 2202 Mobile Adapter Power Consumption

Here are the 2202 **power consumptions** for different states:

1) Transmit Mode : 690mA @ 3.3V (2277 mW) max
2) Receive mode: 360mA @ 3.3V (1188 mW) max
3) Power save mode: 20mA @ 3.3V (66 mW) max

2.7.3.1 Idle Client Usage Profile

The following graph shows the average power consumption for a power save power duty cycle over a range of 90% to 100% and a transmit duty cycle from 0% to 1%. It shows for a transmit duty cycle of 0% that the average power consumption will vary from 38mAh to 53mAh for a respective power save duty cycle range of 95% to 90%. For a transmit duty cycle of 1% the average power consumption will vary from 48mAh to 63mAh. Given a 1300mAh battery, an idle client will consume approximately 30% of the battery.



2.7.3.2 Typical Client Usage Profile

2.7.3.3 Heavy Client Usage Profile

2.7.4 PDA Power Consumption

2.7.5 Synchronization

Stations need to keep synchronization, this is needed for keeping hopping synchronized, and other functions like Power Saving. On an infrastructure BSS this is performed by all the stations updating their clocks according to the AP's clock, using the following mechanism:

The AP transmits periodic frames called Beacon Frames, these frames contain the value of the AP's clock on the moment of the transmission (note that this is the moment when the transmission really occurs, and not when it is put in the queue for transmission, since the Beacon Frame is transmitted using the rules of CSMA, thr transmission may be delayed significantly).

The receiving stations check the value of their clock at the receiving moment, and correct it to keep synchronizing with the AP's clock, this prevents clock drifting which could cause loss of synch after a couple of hours of operation.

2.7.6 Beacon, TIM and PS-Poll Operation

The client will wake up to receive every Beacon transmission from the AP. This interval is programmable and may be selected by the client to be as large as the 802.11 Listen Interval sent by the client in the 802.11 Association Request. The client will examine the bit in the TIM that corresponds to its Association ID. If the client's bit in the TIM is set, the client shall send a PS-Poll frame to the AP to retrieve the frame buffered by the AP that is indicated by the TIM bit. The client shall continue to send a PS-Poll frame to the AP for each subsequent Data frame that is received with the More Data bit set or shall transition to the Active state to allow the AP to send all buffered frames to the client. The client may transition back to the power conservation state at any time after it determines there are no further frames buffered at the AP. To remain in the power conservation state while retrieving buffered frames from the AP, the client shall transmit the Power Management bit as a one in the PS-Poll frame.

When the client sends a PS-Poll to the AP to retrieve a buffered frame, the AP will deliver one frame for each PS-Poll frame received, while the client indicates that it is still in the power conservation state by transmitting the Power Management bit as a one in the Frame Control field of the PS-Poll frame. If there is a frame buffered for the client when the PS-Poll is received, the AP will deliver that frame. This is shown in Figure 1, when polling is done after a TIM, and in Figure 2, when polling is done without checking the TIM. If no frames are buffered for the client when the PS-Poll is received, the AP will send a Null-Data frame to the client. If the AP receives any frame from the client with the Power Management bit sent as a zero, the AP will immediately schedule all frames buffered for the client to be transmitted (consistent with the current QoS parameters for the associated client) and indicate in its internal data structures that the client is now in the active state. In the active state, the AP may transmit any frame received for the client at its earliest opportunity.

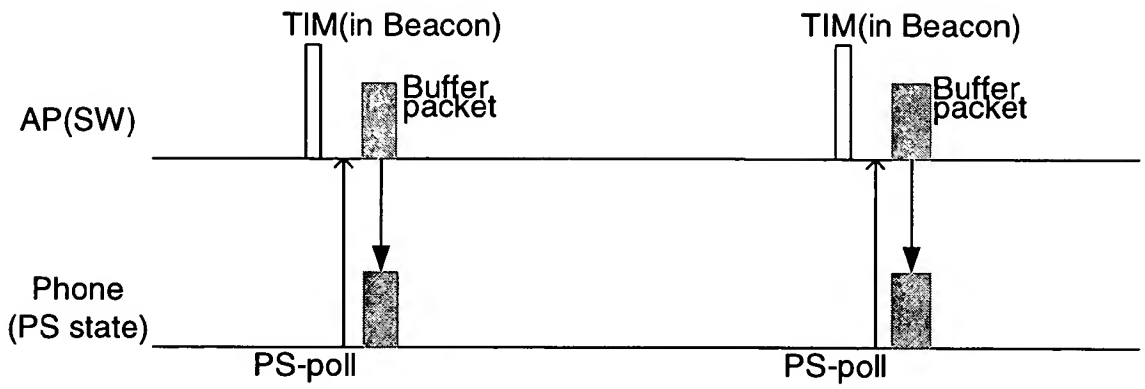


Figure 2-2, PS-Poll after TIM

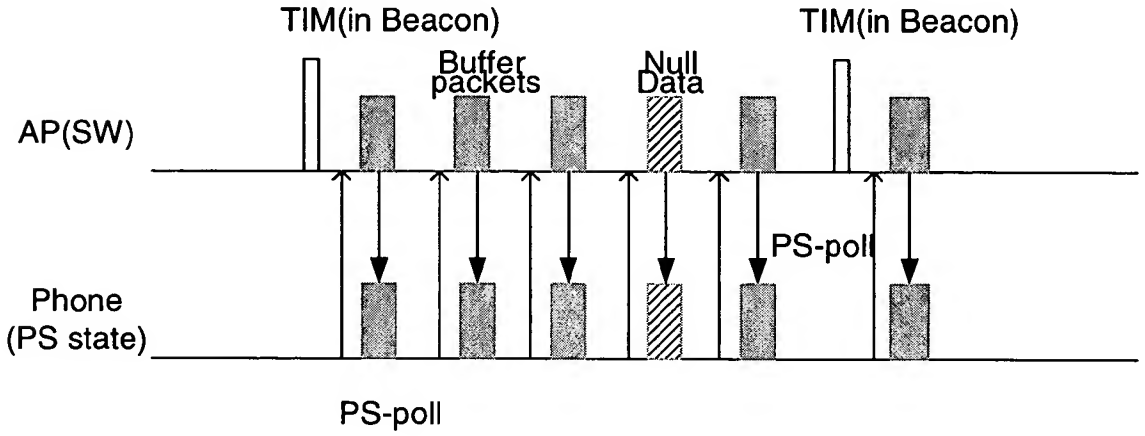


Figure 2-3, PS-Poll Without Checking TIM

2.7.7 Asynchronous PS-Poll Operation

The client may also send a PS-Poll frame to the AP at any time, without regard to whether the client's TIM bit is set.

2.7.8 Power State Transitions

The client may transition from the power conservation state to the active state, by transmitting the Power Management bit as a zero in the Frame Control field of the PS-Poll frame or in any other frame sent to the AP for which an 802.11 ACK frame is required to be sent and the client has a valid Association ID.

The client may transition from the active state to the power conservation state by transmitting the Power Management bit as a one in the Frame Control Field of any frame sent to the AP for which an 802.11 ACK frame is required to be sent and the client has a valid Association ID.

2.8 Client API

2.8.1 Introduction

In order to help troubleshoot wireless network problem, an API to the radio card is required that enables logging to provide status and statistical information about the radio driver directly from the driver whenever an error condition occurs, and then print that information out to a log file. This document is **NOT** a specification but an indicator to the types of API calls that may be made. A review of the actual parameters that are called needs to be reviewed.

2.8.2 Conditions Triggering Logging

The logging should commence with certain predetermined triggers outlined below. The logging will be a configurable such that it can be turned off via a configuration file when no longer required. The information will be logged when any of the following mobile unit application events occur:

- Two Tokens missed – When the handheld misses two tokens (this is during a disconnect but before a token timeout actually occurs). A token is considered missing when one is not received after 30 seconds. We will log the radio card information when the second token is missed; that is 60 seconds without receiving a token request.
- Token Timeout – This is when the handheld misses three tokens, closes the socket, and begins the reconnect process.
- Network Swap – This is during the reconnect process, after connections to all servers on the primary network have failed, and the handheld is about to try the secondary network.
- Network Error – This is when the handheld cannot connect to any server on both the primary and secondary networks.
- Send Error – This is when the TCP/IP returns an error after trying to send data.
- Receive Error – This is when the TCP/IP returns an error after trying to receive data.
- Successful Sign On – This is the only time that the information will be logged for a non-error condition. This log will be done for the sake of comparison, so that there will be set of logs obtained under normal condition to compare error condition logs to.

2.8.3 Parameters to be Logged

The information for each section is obtained by making a separate call to the radio card API.

Get Adapter Firmware Version

This section logs a version string for the adapter's firmware.

Get Adapter Interrupt State

This section logs the current interrupt state of the adapter (enabled or disabled)

Get Adapter MAC Address

This section logs the MAC Address of the current adapter

Get Adapter Net ID

This section logs the current ESSID of the adapter.

Get Adapter Option Flags

This section logs some of the current option configurations. These option include the following

- Override self-broadcast filter
- Send broad/multicast w/o Ack
- Enable MAP destination filter
- Enable reception of broad/multicast when host is powered down.

Get Adapter Power Down State

This section logs the current power state of the adapter (*asleep* or *not asleep*)

Get Adapter Power Mode

This section logs the current power setting of the adapter (CAM or PSP)

Get Adapter Statistics

This section logs many internal statistics that must be kept by the radio card driver. These statistics may include the following:

- # of requested Host Tx's
- # of successful Directed Tx's
- # of successful Non-Directed Tx's
- # of successful Beacon Tx's
- # of successful Poll Tx's
- # of failed Tx's, even after retries
- # of Tx errors due to Ack
- # of Tx errors due timeout waiting for Ack
- # of Tx errors due to missing Ack
- # of Tx errors due to destination address in Ack
- # of Tx errors due to CRC error
- # of Poll errors due to destination address mismatch
- # of Tx's where Tx retry threshold was exceeded
- # of Rx CRC errors
- # of frames dropped due to no buffers
- Source Address not in Association Table
- ESSID does not match MAP's ESSID
- Poll but no data queued
- # of PSP TIM's received
- # of PSP DTIM's received
- # of timeouts waiting for Beacons
- # of timeouts waiting for Poll response
- # of timeouts waiting for the last broadcast/multicast in PSP mode
- Time of first AP Association
- Time of last AP Association

- % missed Beacons in the last ? seconds
- % Tx retries in the last ? seconds
- AP Table entry for the currently Associated AP
- # of AP's described in the AP Table
- Linked list of available AP's
- # of AP Associations
- # of failed AP Associations
- # of failed Association responses
- # of full scans performed
- # of partial scans performed
- Peak RSSI for the Associated AP
- RSSI value at which a PSS is triggered
- # of RSSI Trigger resets

Association. cause:

- AP RSSI fell below the eligible threshold
- Association dropped by the AP (Probe Response)
- Poor Rx/Tx quality
- AP load leveling
- Power mode change
-

Partial scan series cause:

- Unassociated
- RSSI dropped? counts from the peak
- Poor Rx/Tx quality
- AP load leveling

Results of the last self-test
Current power mgt. Mode 0=CAM, 10=PSP
TIM interval algorithm number
Minimum TIM listen interval
Maximum TIM listen interval
Country code: 1=US etc.
Beacon interval
Antenna diversity state: 0=enabled, 1=disabled
# of times FLASH was updated
# of Beacon intervals between DTIM's
Current frequency
Successful null data tx's
Successful authentication tx's
Successful Association tx's
Successful Association response tx's
Successful de-authentication tx's
Successful disassociation tx's
Successful probe tx

Successful probe response tx
Successful RTS
Successful CTS
Duplicate messages
Authentication phase fail
Authentication response phase fail
Association. cause: ESSID change
Association. cause: Preferred/Mandatory change
Operating mode
Association events/status
Number of Associated MUs
Diagnostic program counter
Tx power dBm / mw)
Current Tx rate
Maximum Tx rate
Maximum Associated Tx rate
Adapter BSSID (MAC address)
BSSID of the preferred AP
BSSID of the mandatory AP
Country code (text)
Firmware version string
ESSID string
AP Table
Access control list (MAP only)
MU Association Table (MAP only)
Roaming event log
Firmware version string
Firmware date string
BSSID of Associated AP

Get Adapter Time

This section logs the current adapter time.

Get AP Table

This section returns information about all known AP's. The information provided for each AP follows:

- links entries in used or unused lists

entry AP status

- MU Associated with the AP
- AP Table entry is in use
- entry ineligible due to rate mismatch
- Previous Association. produced poor quality
- age-out counter for the AP entry

the AP's AP_ID
channels from Probe Response
time when Probe Response Rx-ed (LSW)

time when Probe Response Rx-ed (MSW)
IEEE/MAC address of AP adapter
Beacon interval (1 MS LSB)
time offset to next Beacon (1 us LSB)
AP name (ASCII string)
RSSI of Probe received by AP
RSSI of Probe Response Rx-ed by MU
ESSID of the responding AP
Count of Associated MUs
Effective traffic load
RSSI at time of poor Tx/Rx quality
index into RSSI matrix
last n RSSI values
current sum of RSSI matrix

Get Associated AP ID

This section logs the AP ID of the AP to which the device is currently associated.

Get Associated AP MAC Address

This section logs the MAC address of the AP to which the device is currently associated.

Get Associated Status

This section logs the devices current associated state (Associated, Not Associated, or Roamed)

Get Beacon Parameters

This section logs the beacon algorithm min and max values (power saving settings)

Get Device Manufacturing Information

This section logs information about the radio, including Manufacturing ID, Adapter Model Number, Firmware Version/Date, and Adapter Serial Number.

Get Functional Mode

This section logs whether the adapter is operating infrastructure or ad-hoc mode.

Get Mandatory AP ID

This section logs the mandatory AP ID.

Get Least Preferred AP ID

This section logs the least preferred AP ID.

Get Least Preferred AP MAC Address

This section logs the least preferred AP MAC address.

Get Media Configuration

This section logs network configuration parameters, including the following:

- Driver extension version #
- Adapter interrupt number
- Adapter I/O port base address
- Adapter Memory base address
- Adapter Memory size
- Adapter Attribute Memory base address
- Adapter Attribute Memory size
- PCMCIA controller base address
- Allowable packet filters
- Adapter addressing mode (memory/IO)
- Memory mode
- I/O mode
- Adapter card type
- Antenna diversity setting
- Rx receive signal strength indicator (RSSI)
- Rx current channel (frequency)
- Tx status

Get Preferred AP ID

This section logs the preferred AP ID.

Get Radio Link Speed

This section logs the rate of the last transmission

Get Restart Count

This section logs the restart counter value.

Get Roaming Configuration

This section logs the roaming setup of the radio card. The roaming setup includes the following:

- Preferred/Mandatory Access Point BSSID.
- Min. time between re-Associations (sec.)
- Min RSSI
- Tx Quality

Get Supported Data Rates

This section logs the supported data rates on the client adapter.

Self Test – (Execute and Get Results)

The API call will command the adapter to execute a self-test and then read and print the results.

Failure conditions that can be found by this test include:

- ROM checksum failure
- Rx / Tx failure
- DMA failure
- Radio ASIC failure

- Real time clock failure
- Timer and Interrupt failure
- RAM test failure

2.9 Support for the new UNII channels

2.10 Windows CE Port

3 Frame Formats

To implement the functions described in the requirements section of this specification, extensions to several 802.11 MAC Management frames are required. This section describes the new frame formats and the new information element used to implement many of the functions required. In particular, the Beacon, Probe Response, Association Request, Reassociation Request, Association Response, Reassociation Response, and Disassociation frames will now carry a new information element, the Vendor-specific information element. Each of these frames will be described. In addition, the format and content of the Vendor-specific information element will be described.

3.1 Beacon and Probe Response Frames

The Beacon and Probe Response frames will both add the Vendor-specific information element following all information elements defined to be present in the frames by the 802.11 standard and its amendments. The Vendor-specific information element may appear more than once in a frame. The Beacon and Probe Response frames may include the WLAN Capabilities and AP Details information elements.

3.2 Association and Reassociation Request Frames

The Association Request and Reassociation Request frames will both add the Vendor-specific information element following all information elements defined to be present in the frames by the 802.11 standard and its amendments. The Vendor-specific information element may appear more than once in a frame. The station also includes the AP details information element, which includes the mobility domain and address information which the station received in the previous successful association.

3.3 Association and Reassociation Response Frames

The Association Response and Reassociation Response frames will both add the Vendor-specific information element following all information elements defined to be present in the frames by the 802.11 standard and its amendments. The Vendor-specific information element may appear more than once in a frame. The association and reassociation response frames may include the Roaming Candidate AP List and WLAN Capabilities information elements.

3.4 Disassociation Frames

The Disassociation frame will add the Vendor-specific information element following the Reason Code defined to be present in the frames by the 802.11 standard and its amendments. The Vendor-specific information element may appear more than once in a frame.

3.5 Vendor-specific Information Element

The Vendor-specific information element is a standard information element defined in 802.11 where the Element ID value of 221 (0xdd) has been allocated by the 802.11 working group to designate an information element that may be used for carrying proprietary information. The 802.11 working group requires that the first three bytes following the Length be the OUI (IEEE-assigned Organizational Unique Identifier) of the vendor that has defined the particular information element being transmitted. The format of the Vendor-specific information element is shown in the following figure.

ELEMENT ID (221)	LENGTH	OUI	INFORMATION FIELD
1 BYTE	1 BYTE	3 BYTES	N BYTES

Figure 3-1, Vendor-specific Information Element Format

For all Vendor-specific information elements described in this specification, the value of the OUI field will be 0x000b85. For all Vendor-specific information elements where the OUI is 0x000b85, the first byte of the Information Field will be the Sub-element ID. The following table describes the allowable values for the sub-element ID.

SUB-ELEMENT ID	DESCRIPTION
0	RESERVED
1	STA LIST OF APS
2	ROAMING CANDIDATE AP LIST
3	RESERVED
4	WLAN CAPABILITIES
5	AP DETAILS
6-255	RESERVED

Table 3-1, Sub-element ID Values

3.5.1 STA List of APs Information Element

The STA List of APs information element is used by a STA to indicate the APs with which the STA can communicate and the quality of that communication. The format of the information element is shown in the table below.

Length (bytes)	Description
1	Element ID (221 = Vendor-specific information element)
1	Length (number of bytes following this field = 5 + (n * 10))
3	OUI (0x00, 0x0b, 0x85)
1	Sub-element ID (STA List of APs = 1)
1	Number of AP descriptors (n)
n * 10	AP descriptors 1 through n

Table 3-2, STA List of APs Format

Length (bytes)	Description
6	BSSID of AP
1	PHY Type
1	Channel number of AP from Probe Response
1	Signal strength (dBm)
1	Signal quality (SNR, dB)

Table 3-3, AP Descriptor Format

The fields of the Candidate AP Descriptor are defined as follows.

BSSID: This is the 48-bit MAC address of the AP.

PHY Type: The value of this field indicates the PHY type on which the associated BSSID was discovered. The values for PHY Type are shown in the following table.

PHY Type	PHY
0	802.11b
1	802.11a
2	802.11g (OFDM channel)
3-255	Reserved

Table 3-4, STA List of APs PHY Type

Channel number: This is the channel number, as defined for the PHY and country code on which the information element is transmitted. For example, when transmitted on an 802.11b PHY in the US country code, the channel number will be 1 through 11, inclusive. In the JP country code, the channel number will be 1 through 14, inclusive.

Signal strength: This is the value, in dBm of the signal strength of the last transmission from the client received by the AP described by the descriptor.

Signal quality: This is the value, in dB of the signal to noise ratio (SNR) of the last transmission from the client received by the AP described by the descriptor.

3.5.2 Roaming Candidate AP List Information Element

The Roaming Candidate AP List information element is used by the switch/AP to indicate to the STA which other APs will accept an association request or reassociation request from the STA. The format of the information element is shown in Table 4. The Candidate AP Descriptor format is shown in Table 5.

Length (bytes)	Description
1	Element ID (221 = Vendor-specific information element)
1	Length (number of bytes following this field = 5+ (n * 13)))
3	OUI (0x00, 0x0b, 0x85)
1	Sub-element ID (Roaming Candidate AP List = 2)
1	Number of Candidate AP Descriptors (n)
n * 13	Candidate AP descriptors 1 through n

Table 3-5, Roaming Candidate AP List Format

Length (bytes)	Description
6	BSSID of candidate AP
1	PHY Type
1	Channel number
1	Local subnet indicator (local subnet = 0, foreign subnet = 1, same switch= -2, unknown = -1)
1	Signal strength of last reception from STA (dBm)
1	Signal quality of last reception from STA (SNR, dB)
1	Time since last reception from STA (seconds)
1	Load factor (%)

Table 3-6, Candidate AP Descriptor Format

The fields of the Candidate AP Descriptor are defined as follows.

BSSID: This is the 48-bit MAC address of the AP

PHY Type: The value of this field indicates the PHY type on which the associated BSSID was discovered. The values for PHY Type are shown in Table 6.

PHY Type	PHY
0	802.11b
1	802.11a
2	802.11g (OFDM channel)
3-255	Reserved

Table 3-7, Candidate List of APs PHY Type

Channel number: This is the channel number, as defined for the PHY and country code on which the information element is transmitted. For example, when transmitted on an 802.11b PHY in the US country code, the channel number will be 1 through 11, inclusive.

Local subnet indicator: The local subnet indicator value of -2 that the AP described by the descriptor is on the same switch as the AP the client is associated with.

Signal strength: This is the value, in dBm of the signal strength of the last transmission from the client received by the AP described by the descriptor. If there is no information on the last transmission received by the AP, the value of this field shall be -127.

Signal quality: This is the value, in dB of the signal to noise ratio (SNR) of the last transmission from the client received by the AP described by the descriptor. If there is no information on the last transmission received by the AP, the value of this field shall be -127.

Time: This is the value, in seconds, of the time since the last transmission from the client was received by the AP described in the descriptor. Values from 0 to 254 indicate the time since the last transmission was received. A value of 255 indicates the value is not valid.

Load factor: This is the value, in per cent, of the load carried by the AP described in the descriptor.

3.5.3 WLAN Capabilities

The WLAN Capabilities information element is used by the Airespace switch and AP to indicate the features and functions present in the WLAN that a client device, such as a client, can make use of. The format of the information element is shown in Table 7.

Length (bytes)	Description
1	Element ID (221 = Vendor-specific information element)
1	Length (number of bytes following this field = 5)
3	OUI (0x00, 0x0b, 0x85)

1	Sub-element ID (WLAN Capabilities = 4)
1	Capabilities (bit significant)

Table 3-8, WLAN Capabilities Format

There is a single field specific to this information element.

Capabilities: This field is a variable length bit field. The bit field is segmented at each byte boundary to prevent ambiguity in the transmission order as the bit field expands as new capabilities are included in the system. Each bit of this field has significance independent of any other bit in the field. The format of the field is shown in Table 8.

Byte	Bit	Description
0	0	Proxy ARP
0	1	Platinum Queue/Dynamic QoS
0	2	Cooperative Handoff
0	3	Single Authentication
0	4	Picocell
0	5-7	Reserved (transmit as 0, ignore on reception)

Table 3-9, Format of the Capabilities Field

The bits of the Capabilities field are defined below.

Proxy ARP: When the value of this bit is 1, the switch/AP provides proxy ARP service for associated client devices. When the value of this bit is 0, no proxy ARP service is provided.

Platinum Queue/Dynamic QoS: When the value of this bit is 1, the switch/AP provides dynamic QoS using the Vendor-specific information element and reassociation of the client device. When the value of this bit is 0, no dynamic QoS service is provided.

Cooperative Handoff: When the value of this bit is 1, the switch/AP provides cooperative handoff services using the Vendor-specific information element. When the value of this bit is 0, no cooperative handoff service is provided.

Single Authentication: When the value of this bit is 1, the switch/AP provides single authentication services for 802.1X as the client roams from one AP to another in the same mobility group. When the value of this bit is 0, no single authentication service is provided.

Picocell: When the value of this bit is 1, the switch and AP is operating in picocell mode. In picocell mode, load balancing is performed by the client, based on the Roaming Candidate AP List and either active or passive scanning by the client. The switch/AP will not reject an association/reassociation attempt in picocell mode.

3.5.4 AP Details

The AP Details information element is used to announce information about the AP and its associated switch. The client will use this information when roaming from one AP to another. The format of the information element is shown in Table 12.

Length (bytes)	Description
1	Element ID (221 = Vendor-specific information element)
1	Length (number of bytes following this field = 13)
3	OUI (0x00, 0x0b, 0x85)
1	Sub-element ID (AP Details = 5)
1	Load Factor (%)
8	Mobility Group Identifier
4	Controller Address

Table 12, AP Details Format

The fields of the AP Details information element are defined as follows.

Load factor: This is the value, in per cent, of the load carried by the AP described in the descriptor. This value is ignored when the IE is included in the station's Association Requests

Mobility Group Identifier: This is a unique value that identifies all of the switches, and the APs that are connected to these switches, in a common mobility group.

Controller Address: This is the IP address of the AP (or controller in a hierarchical system)

3.5.5 Station Details

The Station Details information element is used to announce information about the AP and its associated switch. The station will use this information when roaming from one AP to another. The format of the information element is shown in Table 11.

Length (bytes)	Description
1	Element ID (221 = Vendor-specific information element)
1	Length (number of bytes following this field = 13)
3	OUI (0x00, 0x0b, 0x85)
1	Sub-element ID (Station Details = 6)
4	Hand-off Counter
8	Mobility Group Identifier
4	Controller Address

Table 11, Station Details Format

The fields of the Station Details information element are defined as follows.

Hand-off Counter: This counter maintained by the station and is monotonically increased upon every association request.

Mobility Group Identifier: This value is sent to the station in the AP Details IE and is cached by the station when it successfully associates with an AP.

Controller Address: This value is sent to the station in the AP Details IE and is cached by the station when it successfully associates with an AP.

4 Custom Client Test Plan

This section describes a series of tests to verify the custom client design. Table 4-1 lists the tests and the order in which they will be executed in the Blue Room to verify that the custom client driver functions. Tests 1 – 7 do not require the fast roaming portion of the driver. Tests 1 – 4 are designed to verify and optimize the transmit power and receiver sensitivity. Tests 5 – 6 are designed to verify some of the basic design assumptions of the fast roaming algorithm. Test 7 is design to verify the capacity of an access points. Tests 8-16 require the fast roaming feature and are designed to incrementally verify the functionality of the fast roaming feature.

#	Test	Time	Tools	Goal / Description
1	Coverage Test	3 hrs	Ekahau	Verify the coverage of final deployment.
2	SNR / Cell Size	2 hrs	Client	Verify how fast SNR changes while walking and verify cell size
3	AP Isolation	4 hrs	AeS	Verify the isolation between Co-channel APs
4	CoChannel Inter.	4 hrs	Chariot	Verify we can ignore weak packets. Chariot- filesndl
5	Roaming List	4 hrs	AeS Ekahau	Verify a validate roaming candidate is on the list. This test will use the results of the coverage test
6	Roaming Selection	2 hrs	Client AeroPeek	Verify we can find the right roaming candidate. Aeropeek will be used to measure probe response time and missed probes.
7	AP Capacity	5 hrs	Chariot	Verify AP capacity vs. # of users vs. packet size. Chariot- filesndl
8	Mobility Test 1 (AP)		Chariot	Verify mobility with a single client, single WSS, No WPAII. Chariot- QOS script/TBD
9	Mobility Test 2 (WSS)		Chariot	Verify mobility with a single client, multiple WSS, No WPAII Chariot- QOS script/TBD
10	Mobility Test 3		Chariot	Verify mobility and load balancing with multiple clients, multiple WSS, No WPAII
11	Mobility Test 4		Chariot	Verify mobility with a single client, multiple WSS, WPAII

12	Mobility Test 5 (Load Sharing)		Chariot	Verify mobility with multiple clients, multiple WSS, WPAII
13	AP Fail Over		Chariot	Verify AP failover with a single client
14	AP Fail Over		Chariot	Verify AP failover with multiple clients
15	WSS Fail Over		Chariot	Verify WSS fail over with a single client
16	WSS Fail Over		Chariot	Verify WSS fail over with multiple clients

Table 4-1 Custom Client Blue Room Test

4.1 Co Channel Interference Test

4.1.1 Test Objective

The goal of this test is to verify that weak packets can be ignored.

4.1.2 Test Description

This test will consist of running 2 chariot sessions between AP and client pairs in two different test setups. The first test setup shown in figure 4-1 will consist of 2 clients connected to an access point via RF cables, attenuators and RF couplers. The second test setup will consist of 2 clients each associated with different APs on opposite sides of the test lap. Each client will be positioned to have an -60 dBm or better average RSSI to its associated AP. The RSSI between APs will be between -85 dBm to -80 dBm. In both test setups all clients will be running a chariot session. In the RF cable test setup the RF attenuation on client 1 will be increased until the AP can not hear client and the signal the chariot session will be increased . Without the ignore feature turned on the total throughput of both chariot sessions will be equal to that of a single access point. This is because the radios are deferring to each others traffic and sharing the bandwidth. When the ignore feature is turned on both Chariot streams should be equal to that of a single access point.

4.1.3 Test Setup

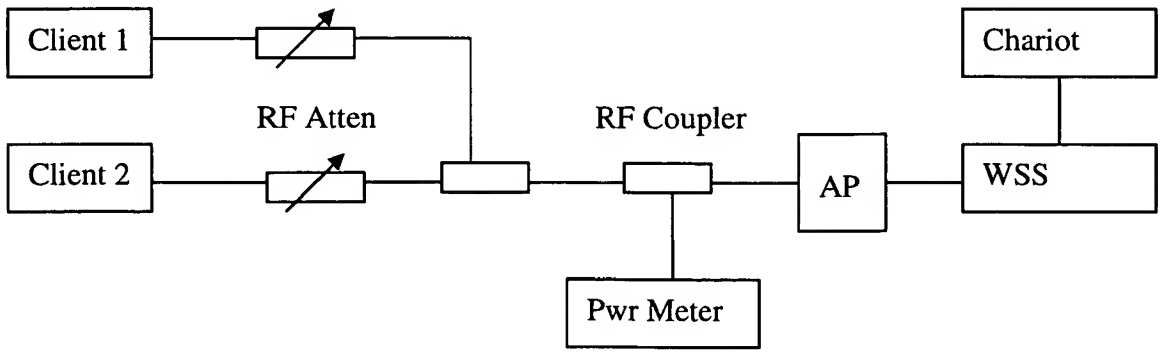


Figure 4-1 Co Channel RF Cable Test Setup

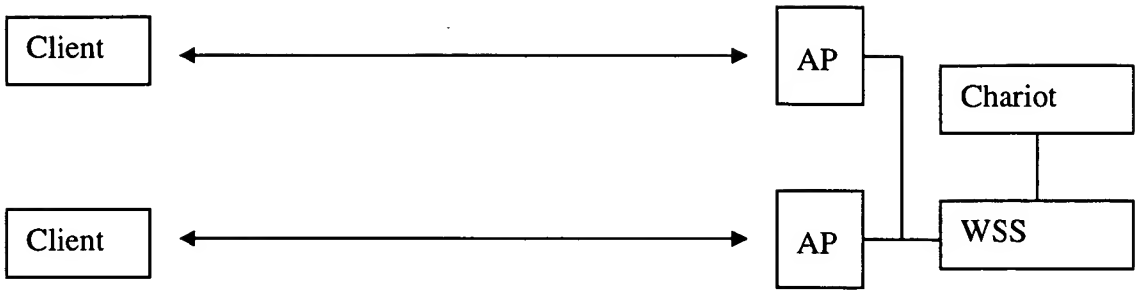


Figure 4-2 Co Channel Lab Test Setup

4.1.4 Test Procedure

4.1.5 Data Analysis / Results

4.2 AP Co-Channel Isolation

4.2.1 Test Objective

The goal of this test is to determine the number of APs which hear each other on a co-channel and also the average amount of power which each co-channel AP hears the other. A NxN matrix is created to show if what amount of N pairs actually still hear each other.

4.2.2 Test Description

4.2.3 Test Setup

4.2.4 Test Procedure

With DCA:

1. Enable RRM Group Mode for all Switches
2. Assign a RRM group leader
3. Configure RRM group leader
4. Enter switch CLI, enter commands:

- config 802.11 disable network
- config country us
- config 802.11a enable network
- config 802.11a channel global off
- config 802.11a channel global auto
- debug airwave-director channel enable
- devshell rrmLogDCA(2,0,1)
- devshell rrmLogDCA(2,1,1)

Capture the devshell output to a file

Without DCA:

Within CLI Enter commands:

- debug airwave-director channel enable
- devshell rrmLogDCA(2,1,1)

4.2.5 Data Analysis / Results

4.3 AP Coverage Test

4.3.1 Test Objective

The goal of this test is to perform a Ekahau walkthrough of the floor to not only confirm the level of coverage, but to provide a comparison of infrastructure AP roam list against actual.

4.3.2 Test Description

- Using Ekahau Site Suvey Tool
  - Start Site Survey
  - Select Devices-> Deselect "Use" next to Client Card->in right hand box, scroll down, deselect 11b band.
    - (Ensure only 11a band is selected).
  - File-> New-> Map (Select Floor Map File)

- File-> New-> Survey
- Press Record
- Start Clicking on map every 2-5 feet and keep walking at a constant speed in-between clicks. Verify that the walking path is showing up on screen and do not leave more than a
- To stop\start\pause survey press Record

4.3.3 Test Setup

4.3.4 Test Procedure

4.3.5 Data Analysis / Results

4.4 AP Capacity

4.4.1 Test Objective

The goal of this test is to verify that the latest version of the client driver satisfies the AP capacity requirements in terms of users with small packets.

4.4.2 Test Description

This test will be done in both the pico cell test lab and the Blue Room to verify the capacity of an access point with 1 to 20 users streaming data with packet sizes of 64, 128, 256, 512 1025 and 1400 bytes for RF link rates greater than 36Mbps.

Figure 12-3 is based on actual measurements taken February of 2004 of a single access point supporting RF data link rates of 36Mbps and greater servicing multiple clients for various packet sizes. In all cases the measured exceeded the AP capacity used for planning purposes.

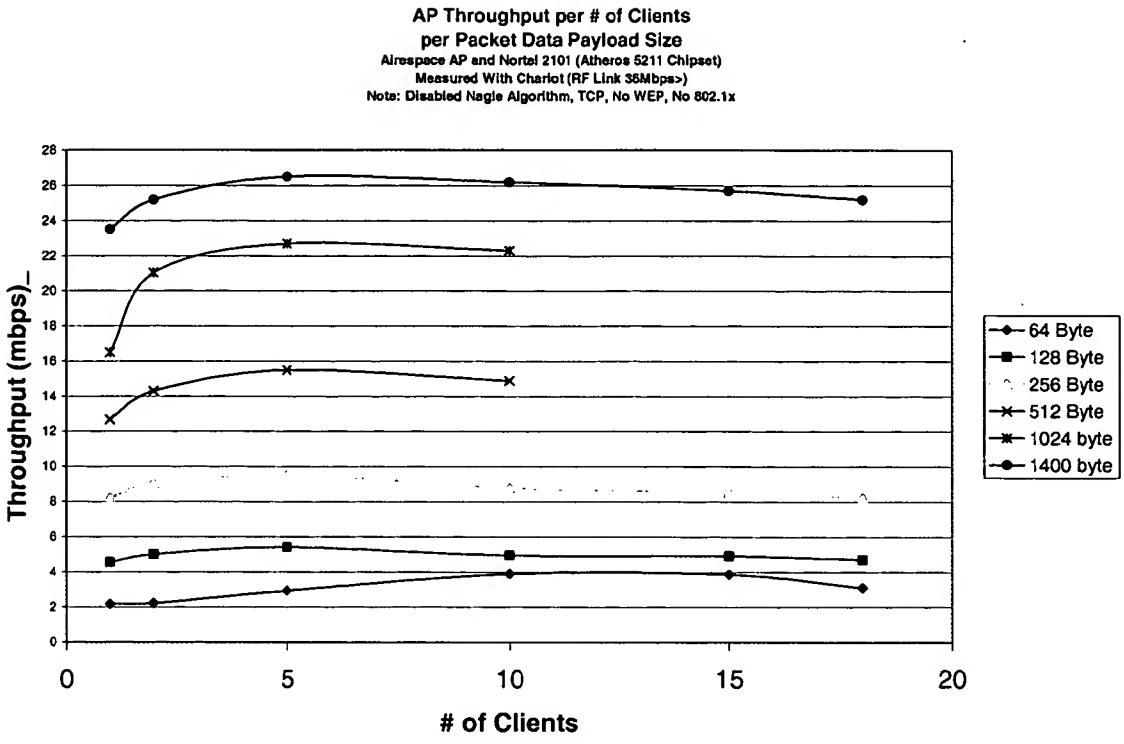


Figure User Throughput vs # of Clients vs. Pkt. Size

Note: The 512 byte and 1024 byte curves are incomplete due to testing time constraints

Table 12-1 shows the difference between the model used for capacity planning purposes and the measured data. It shows that the single user capacity model with 80% efficiency assumption is conservative relative to the measured data for all packet sizes.

Pkt Size	Model[1]		Model with 80% eff. Assumption[2]		Measured Data[2]
	54Mbps	36Mbps	54Mbps	36Mbps	>36Mbps
64 Bytes	3.3	3.14	2.64	2.50	3.1
128 Bytes	6.2	5.8	5.00	4.64	4.7
256 Bytes	11.1	10	8.88	8.00	8.2
1400 Bytes	31.7	24	25.36	19.2	25.2

Table Access Point Capacity

1- The model columns show the predicted user throughput for RF data link rates of 36, 48 & 54 Mbps

2- The measured data columns show the measured access point throughput with 18 clients.

Figure 12-4 shows the variation in user performance for 15 users streaming 128 byte packets. It shows that user performance falls between 253 kbps and 432 kbps for all users.

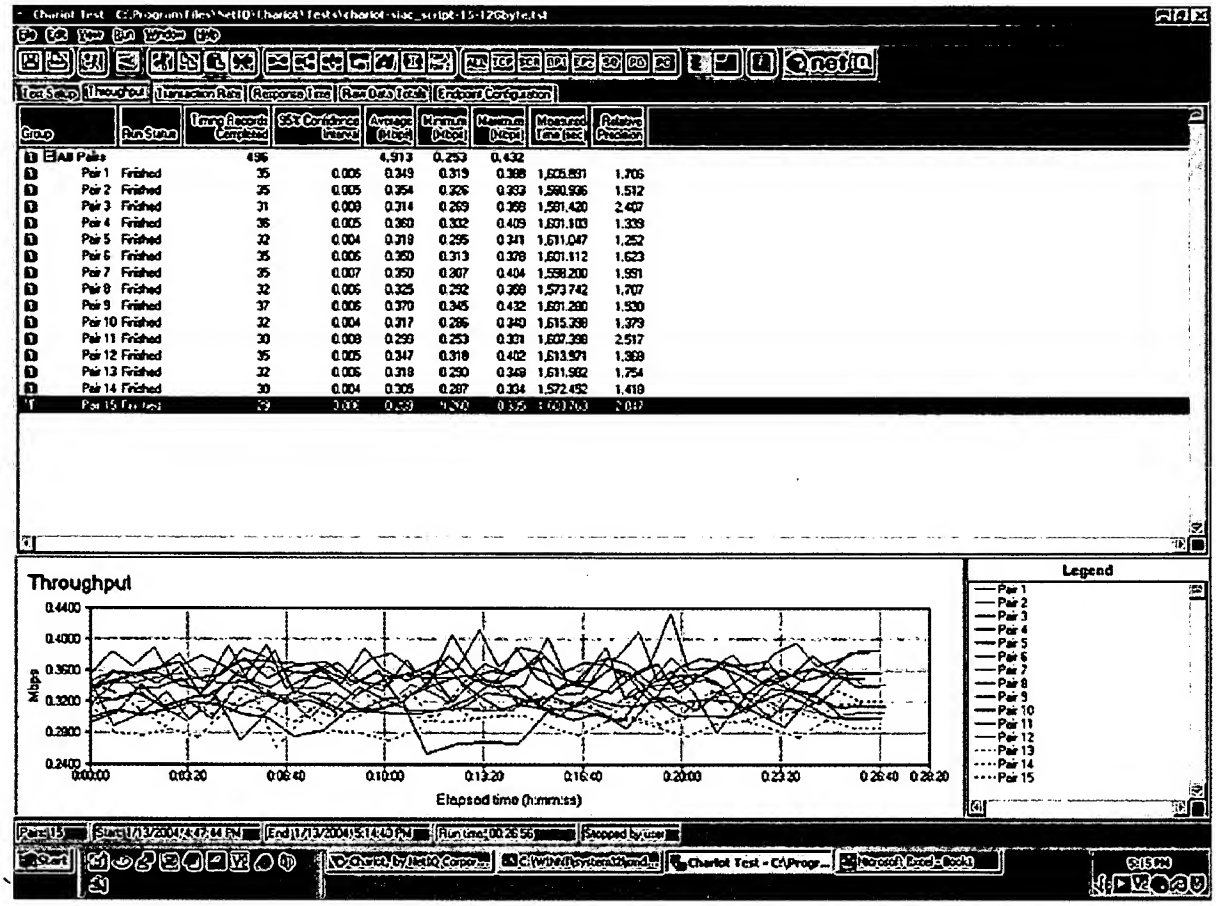


Figure User Throughput for 15 users on a single AP

4.4.3 Test Setup

WS 5000/ Access Port/ Mobile Unit Configuration:

Packet Size (Bytes): 64, 128, 512, & 1518

Encryption (WEP): 128 bit

Key Rotation (TKIP): Yes

MU Power Save Mode: Full

Channel/co-location/overlap: None

Inter-packet Delay (msec): N/A

Number of MUs: 1, 2, 4, 8, 16, 20

Number of Access Ports: 1

User Authentication: RADIUS

Total # of iterations:

Wired Sniffer Activities: NONE

Wireless Sniffer Activities: NONE

4.4.4 Test Procedure

Run the "***Net Latency***" scripts, with multiple values of packet size while increasing the population of MUs associated with the Access Port during each test run. Each script will be identified as "***Lxx***", where "***xx***" denotes the packet size in bytes. The number of MUs will be increased and the test run repeated until the performance degradation as a function of number of MU associations is identified. MU to AP distances will be kept constant throughout all tests. Run three times with RTPtest script.

1) Configure DCA
- Manually Configure DCA giving APs predefined channel assignments
- Enable Automatic DCA **and record channel assignment**

2) Given no DHCP server, configure each client (Chariot endpoint) with a static IP address.

3) Configure AeS CLI command: config advance client-mobility 50

[This forces client to deauth if Client does not ACK after 50]

4) Disable Aggressive Load Balancing / Disable DCA / Set Tx Power = 3 / RRM Timers to Maximum

5) Chariot Configuration (for each of the above)

1. Configure Link Pair Test with IP addresses
2. Use script 'filesndl' for TCP throughput test
    i. Modify Packet Size to 128 bytes
    ii. Disable Nagle Algorithm at the beginning of script
3. Copy the Link Pair Test for Remaining # of Test Client IPs
4. Run Test and Record Throughput,
5. Save results to a chariot file
6. Use script 'xxxxxxx' for UDP latency test
    a. Modify Packet Size to 128 bytes
    b. Disable Nagle Algorithm at the beginning of script

7. Copy the Link Pair Test for Remaining # of Test Client IPs
8. Run Test and Record Throughput,
9. Save results to a chariot file

4.4.5 Data Analysis / Results

- Access Point Throughput vs. # of Clients vs. Packet Size
- Avg Client Throughput vs. # of Clients vs. Packet Size
- Std. Dev. Client Throughtput vs. # of Clients vs. Packet Size
- Avg Client Pkt Delay vs. # of Clients vs. Packet Size
- Std. Dev. Pkt Delay vs. # of Clients vs. Packet Size

4.5 MobilityTest 0- (Cell Size and SNR Characterization)

4.5.1 Test Objective

This test characterizes the changes in SNR as a users walks around the POST. The goal of this test is to

1. Estimate the size of coverage area in both seconds and feet
2. Quantify how fast the SNR changes

4.5.2 Test Description

This test will consist of collecting 10 SNR profiles for the following scenarios

1. Walking straight through the coverage of an access point
2. Walking out of coverage going around the post
3. Walking out of coverage going around a corner on a wall
4. Walking out of coverage going to the next room
5. Walking under\inside a post

4.5.3 Test Setup

WS 5000/ Access Port/ Mobile Unit Configuration:

Packet Size (Bytes): N/A

Encryption (WEP): N/A

Key Rotation (TKIP): N/A

MU Power Save Mode: N/A

Channel/co-location/overlap: None

Inter-packet Delay (msec): N/A

Number of MUs: 1

Number of Access Ports: 1

User Authentication: N/A

Total # of iterations:

Wired Sniffer Activities: NONE

Wireless Sniffer Activities: NONE

4.5.4 Test Procedure

1. Using Intelligraphics Client Driver create the Profile for the SSID, security, and 5GHz band
2. Select Option->Roaming AP List
3. Select Enable Driver Logging and Create a datalog file.
4. Walk around the room and monitor the GUI for transitions and data collection.

4.5.5 Data Analysis / Results

4.6 Roaming List

4.6.1 Test Objective

The goal of this test is to make sure that the roaming list provided by the access point contains a valid roaming candidate for all possible exit points from the coverage area. This test looks at all the neighboring APs seen by each AP and sorts them by SNR and then looks at how long the list needs to be to include all possible roaming candidates.

4.6.2 Test Description

This test will consist of using Site Survey to measure the coverage area of an access point and identifying the possible roaming candidates for each exit point of the coverage area. The list of neighboring APs as seen by the covering AP will be sorted by SNR and the length of the list needed to include at least one roaming candidate at each exit point of the AP's coverage area. The roaming list is sorted by SNR.

4.6.3 Test Setup

4.6.4 Test Procedure

To get the AP Roaming list from each AP enter following command at the switch interface

Show -> AP -> AutoRF -> 802.11a -> [AP Name]

You can also get the AP roaming list from the Web Interface by going to the monitor page.

4.6.5 Data Analysis / Results

4.7 Mobility Test 0- (Roaming List Selection)

4.7.1 Test Objective

The goal of this test is to characterize how long it takes to probe the APs on the roaming candidate list and how many probes it takes to find the correct roaming candidate

4.7.2 Test Description

The test consists of placing the client at 4' off the ground and having the client driver go through the list of APs and send a configurable number of probes to each AP on the list. The list consists of all the APs within 50 feet of the location. For each location all the APs that have an SNR above 30dB in 100 continuous SNR samples will be considered a valid roaming choice. For each l ....

4.7.3 Test Setup

WS 5000/ Access Port/ Mobile Unit Configuration:

Packet Size (Bytes): 128

Encryption (WEP): 128 bit

Key Rotation (TKIP): Yes

MU Power Save Mode: Full

Channel/co-location/overlap: None

Inter-packet Delay (msec): N/A

Number of MUs: 1

Number of Access Ports: 24 - 48

User Authentication: RADIUS

Total # of iterations: 100 per test location

Wired Sniffer Activities: NONE

Wireless Sniffer Activities: Airopeek

Client Software: Custom Client Driver

Chariot: No

4.7.4 Data Results / Analysis

From the Aeropeek data, the Probe request / probe response transaction time is obtained. In addition to probe response times, the number of probe requests that go unanswered needs to be determined.

Figure 4-3 shows data collected in the PicoCell test net for the no load case. It shows a max probe response time of 1.1 msec.

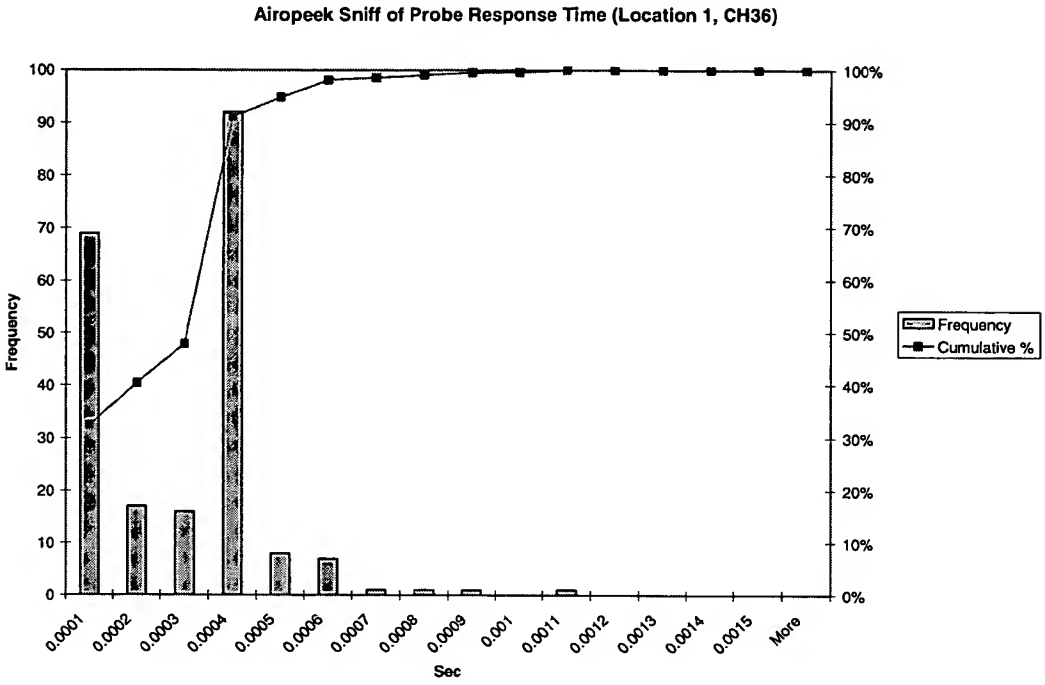


Figure 4-3 Probe Response Time

For each location, valid roaming candidates are defined as any candidate that have an SNR greater than 30dB in 100 continuous SNR samples. For each test location the number of times an invalid candidate is selected is recorded.

Figure 4-4 shows the SNR for all the APs from a given test location. It shows that the AP directly above the test location and the adjacent APs meet the definition of valid roaming candidates. From the list of selected APs, the number of times an invalid roaming candidate can be determined.

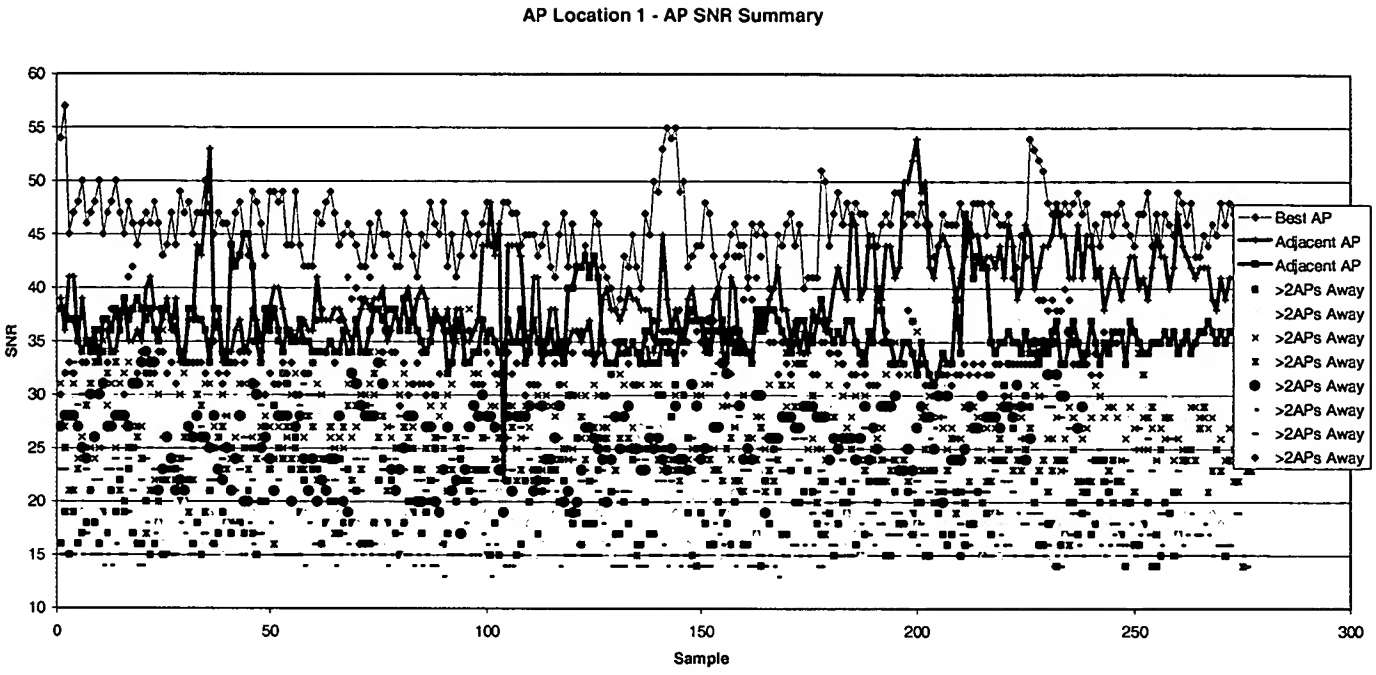


Figure 4-4 AP SNR

4.8 Mobility Test 1 (Single Client, Single WSS, No WPA)

4.8.1 Test Objective

The goal of this test is to verify that a single client can move through a network of access points associated with a single WSS and complete hand offs with a maximum packet delay of 100 msec

4.8.2 Test Description

This test will consist of pushing a plastic cart with a client on it through the network with a chariot session streaming data. Chariot will be configured to measure packet delay. In the client driver, every state transition in the handoff state machine will be time stamped and recorded.

4.8.3 Test Setup

WS 5000/ Access Port/ Mobile Unit Configuration:

Packet Size (Bytes): 128

Encryption (WEP): 128 bit

Key Rotation (TKIP): Yes

MU Power Save Mode: Full

Channel/co-location/overlap: None

Inter-packet Delay (msec): N/A

Number of MUs: 1

Number of Access Ports: 24

User Authentication: RADIUS

Total # of iterations:

Wired Sniffer Activities: NONE

Wireless Sniffer Activities: NONE

Client Utility: YES

Chariot: YES

4.8.4 Test Procedure

1. Start up Chariot Session
2. Start up Client Utility
3. Push Cart through the network until 100 handoffs are recorded on the client utility

4.8.5 Data Results / Analysis

From the Chariot data a histogram of packet delay will be generated.

From the client utility data the time and percentage of time spent in each state will be generated and a histogram and statistics of the time while not in state 1 will be generated.

4.9 Mobility Test 2- (Single Client, Multiple WSS, No WPA)

4.9.1 Test Objective

The goal of this test is to verify that a single client can move through a network of access points associated with 4 WSSs and complete hand offs with a maximum packet delay of 100 msec

4.9.2 Test Description

This test will consist of pushing a plastic cart with a client on it through the network with a chariot session streaming data. Chariot will be configured to measure packet delay. The client driver will record and time stamp every state transition in the handoff state machine.

4.9.3 Test Setup

WS 5000/ Access Port/ Mobile Unit Configuration:

Packet Size (Bytes):	128
Encryption (WEP):	128 bit
Key Rotation (TKIP):	Yes
MU Power Save Mode:	Full
Channel/co-location/overlap:	None
Inter-packet Delay (msec):	N/A
Number of MUs:	1
Number of Access Ports:	24
User Authentication:	RADIUS

Total # of iterations:

Wired Sniffer Activities: NONE

Wireless Sniffer Activities: NONE

Client Utility: YES

Chariot: YES

4.9.4 Test Procedure

- Start Up Chariot Session
- Start up Client Utility
- Push Cart through the network until 100 handoffs are recorded on the client utility

4.9.5 Data Results / Analysis

From the Chariot data a histogram of packet delay will be generated.

From the client utility data the time and percentage of time spent in each state will be generated and a histogram and statistics of the time while not in state 1 will be generated.

4.10 Mobility Test 3- (Multiple Client, Multiple WSS, No WPA)

4.10.1 Test Objective

The goal of this test is to verify that 20 to 100 clients can move through a network of access points associated with 4 to 8 WSSs and complete hand offs with a maximum packet delay of 100 msec. In addition to verifying fast handoff, this test will verify that the client's load balance when making handoffs.

4.10.2 Test Description

This test will consist of pushing plastic carts with 5 to 10 clients on each through the network with a chariot session running on each client streaming data. Chariot will be configured to measure packet delay. The client driver will record and timestamp every state transition in the handoff state machine. Additionally for each handoff the client driver will record the minimum and maximum load factor of all possible roaming candidates that met the SNR requirement and the load factor of the access point selected. ACS will be used to record all access point associations to allow the effectiveness of load balancing.

4.10.3 Test Setup

WS 5000/ Access Port/ Mobile Unit Configuration:

Packet Size (Bytes): 128

Encryption (WEP): 128 bit

Key Rotation (TKIP): Yes

MU Power Save Mode: Full

Channel/co-location/overlap: None

Inter-packet Delay (msec): N/A

Number of MUs: 1

Number of Access Ports: 24

User Authentication: RADIUS

Total # of iterations:

Wired Sniffer Activities: NONE

Wireless Sniffer Activities: NONE

Client Utility: YES

Chariot: YES

4.10.4 Test Procedure

- Start Up Chariot Session
- Start up Client Utility

- Push Cart through the network until 100 handoffs are recorded on the client utility

4.10.5 Data Results / Analysis

From the Chariot data a histogram of packet delay will be generated.

From the client utility data the time and percentage of time spent in each state will be generated and a histogram and statistics of the time while not in state 1 will be generated.

4.11 Mobility Test 4- (Single Client, Multiple WSS, WPAII)

4.11.1 Test Objective

The goal of this test is to verify that a single clients configure with WPAII security can move through a network of access points associated with 4 to 8 WSSs and complete hand offs with a maximum packet delay of 100 msec.

4.11.2 Test Description

This test will consist of pushing plastic carts with 5 to 10 clients on each through the network with a chariot session running on each client streaming data. Chariot will be configured to measure packet delay. The client driver will record and timestamp every state transition in the handoff state machine.

4.11.3 Test Setup

WS 5000/ Access Port/ Mobile Unit Configuration:

Packet Size (Bytes): 128

Encryption (WEP): 128 bit

Key Rotation (TKIP): Yes

MU Power Save Mode: Full

Channel/co-location/overlap: None

Inter-packet Delay (msec): N/A

Number of MUs: 1

Number of Access Ports: 24

User Authentication: RADIUS

Total # of iterations:

Wired Sniffer Activities: NONE

Wireless Sniffer Activities: NONE

Client Utility: YES

Chariot: YES

4.11.4 Test Procedure

- Start Up Chariot Session
- Start up Client Utility
    - Select Options-> Enable Driver Logging (Select)
- Push Cart through the network until 100 handoffs are recorded on the client utility

4.11.5 Data Results / Analysis

From the Chariot data a histogram of packet delay will be generated.

From the client utility data the time and percentage of time spent in each state will be generated and a histogram and statistics of the time while not in state 1 will be generated.

4.12 Mobility Test 5- (Multiple Client, Multiple WSS, WPAII)

4.12.1 Test Objective

The goal of this test is to verify that a single client configured with WPAII security can move through a network of access points associated with 4 to 8 WSSs and complete hand offs with a maximum packet delay of 100 msec.

4.12.2 Test Description

This test will consist of pushing plastic carts with 5 to 10 clients on each through the network with a chariot session running on each client streaming data. Chariot will be configured to measure packet delay. The client driver will record and timestamp every state transition in the handoff state machine.

4.12.3 Test Setup

WS 5000/ Access Port/ Mobile Unit Configuration:

Packet Size (Bytes):	128
Encryption (WEP):	128 bit
Key Rotation (TKIP):	Yes
MU Power Save Mode:	Full
Channel/co-location/overlap:	None
Inter-packet Delay (msec):	N/A
Number of MUs:	1

Number of Access Ports: 24

User Authentication: RADIUS

Total # of iterations:

Wired Sniffer Activities: NONE

Wireless Sniffer Activities: NONE

Client Utility: YES

Chariot: YES

4.12.4 Test Procedure

- Start Up Chariot Session
- Start up Client Utility
    - Select Options-> Enable Driver Logging (Select)
- Push Cart through the network until 100 handoffs are recorded on the client utility

4.12.5 Data Results / Analysis

From the Chariot data a histogram of packet delay will be generated.

From the client utility data the time and percentage of time spent in each state will be generated and a histogram and statistics of the time while not in state 1 will be generated.

>THIS IS **THE WAY**

Next Generation Wireless LAN: NYSE

Presented by:

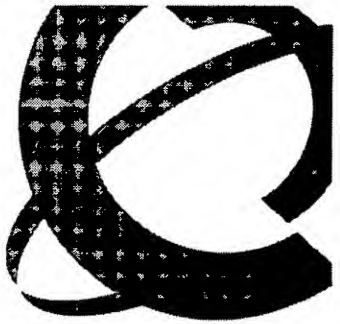
Tom Jencz, Director of Services

Lisa Schwartz, Product Line Management, WLAN

Frank Burke, Ioannis (Yanni) Apostolakos, Service Primes

>THIS IS NORTEL

SIAC Opportunity – Overview

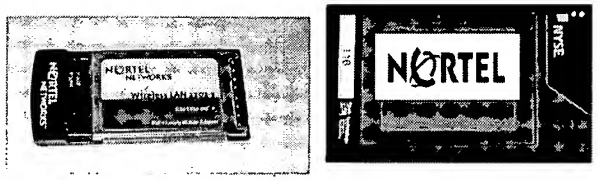


- > Provide a Next Generation WLAN solution for the Securities Industry Automation Corporation (SIAC) for use by the New York Stock Exchange (NYSE)
- > Utilize Adaptive Wireless LAN, Passport 8600, BayStack and Radius architecture to form a Wireless LAN that will replace Symbol antiquated architecture.
- > Implementation on the @45,000 sq. ft. trading floor of NYSE
- > #1 project for the NYSE and SIAC for 2004
- > Unprecedented, cutting edge design and use of 802.11a with many more channels for using multimedia applications
  - Lower Total Cost of Ownership for many users and various different deployment options.

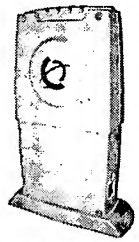
This is the Solution Nortel Sold to NYSE

Nortel Wireless LAN Equipment:

> **WLAN Mobile Adapter 2202** – a 32-bit multimode Cardbus adapter, supporting 802.11b/g and 802.11a.

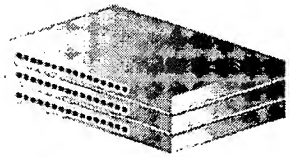


> **Nortel WLAN 22XX Access Point** – a tri-mode LightWeight Access Point that supports 802.11b, g and 802.11a and is capable of roaming seamlessly between the three frequency bands.

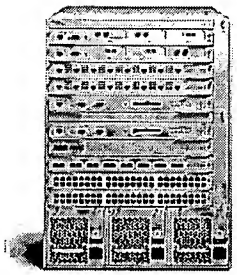


> **Nortel WLAN 2270 Security Appliance** – a Security Appliance to protect and manage mobile communications transmitted over the wireless LAN.

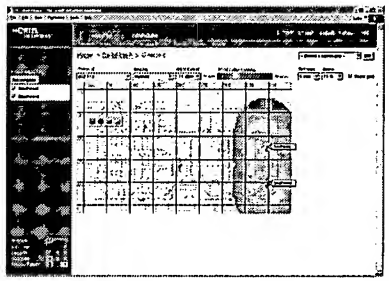
> **BayStack 460 POE Switch** – a Layer 2 switch (with L2 - L4 QOS and Filter capability) that provides power over Ethernet to all APs.



> **Passport 8600 L2/L3 Routing Switch** – a Layer 2 – 3 routing switch that provides the CORE wire speed connectivity between the solution components.



> **Wireless Management System** – To centrally managed the Wireless Network

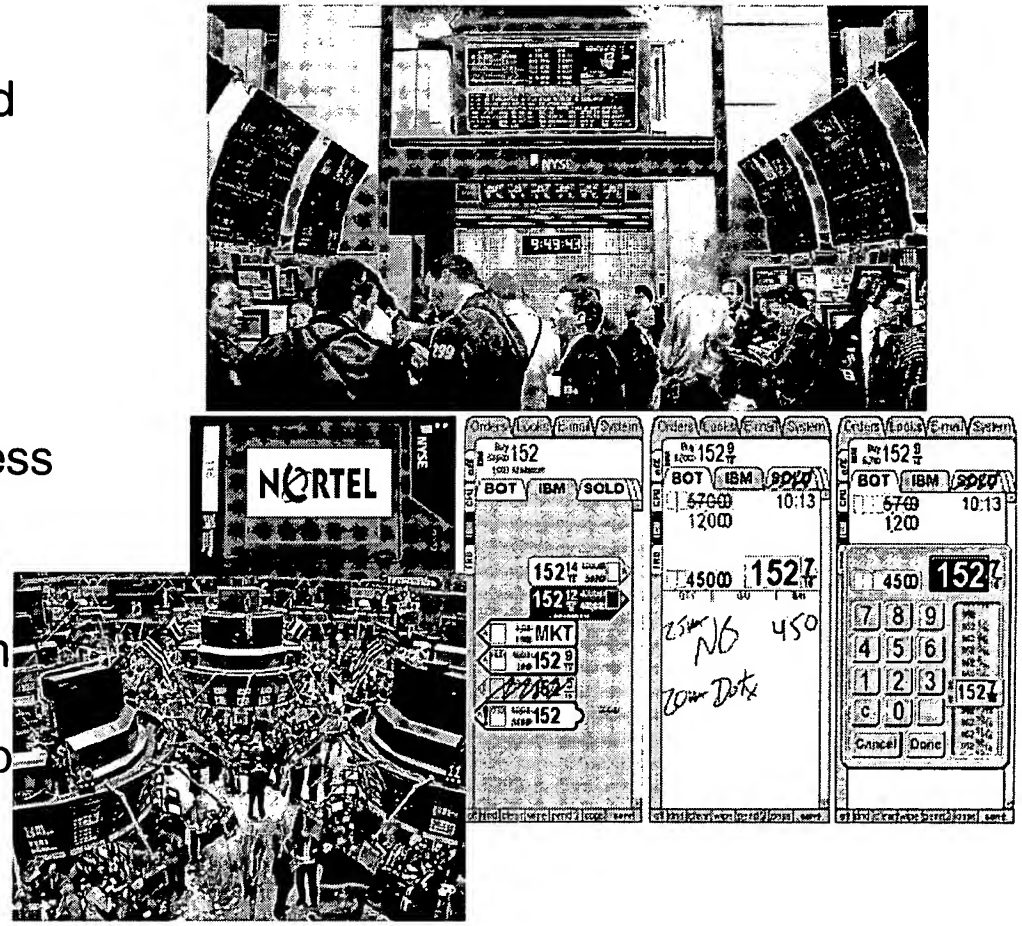


NYSE: Next Generation WLAN

> High Performance
- Instant Trades with guaranteed throughput
- Continuous uptime

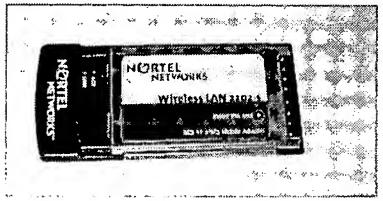
> Security
- Standards Based for low cost
- Nortel customized Mobile Adaptor and Switch for seamless and fast handoff

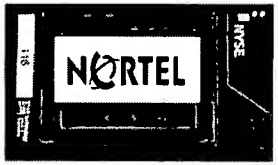
> Reliability – High Throughput
- Full network redundancy which eliminates points of failure
- Provides guaranteed service to many Fast Roaming users

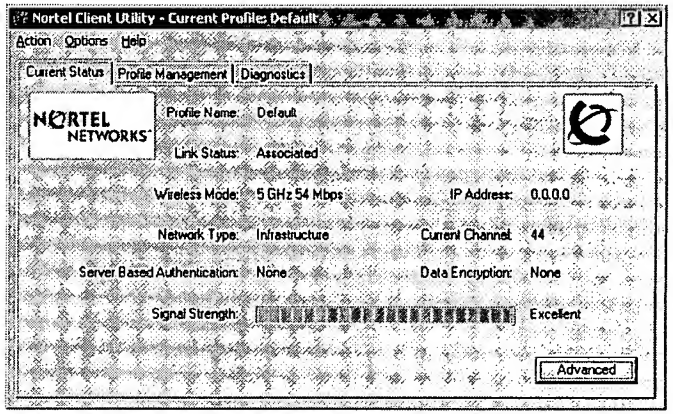


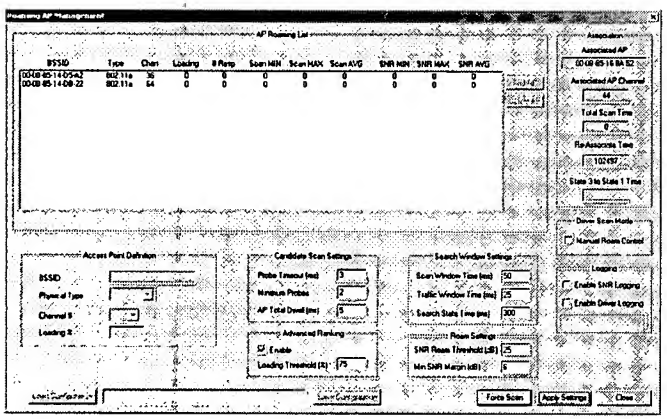
>THIS IS **THE WAY** **Nortel Has changed Wireless LAN**

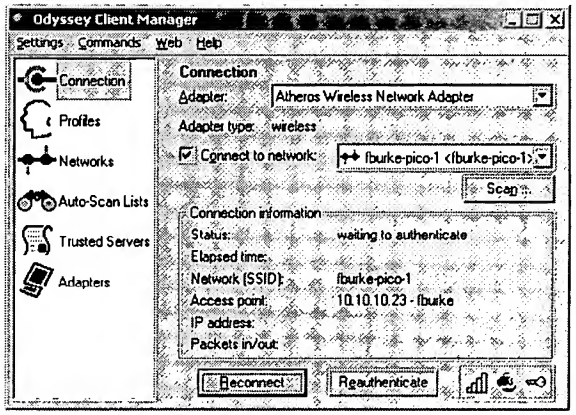
This is the Way...Nortel Does Wireless Security for the NYSE



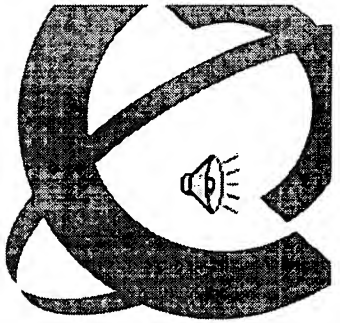








Benefits of NYSE: Next Generation Wireless Network

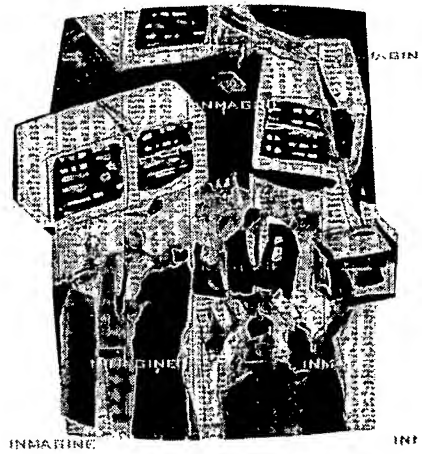


> Fully Redundant to Core
- High-density, AP clustering
- Passport Network Strength with SMLT

> Centralized security
- Standards-based with added Nortel IPR for fast handoff
- Intelligent key management across APs, switches and mobility groups
- Nortel Core Network Firewall

> Centralized Management
- Easy to Use Centralized Management

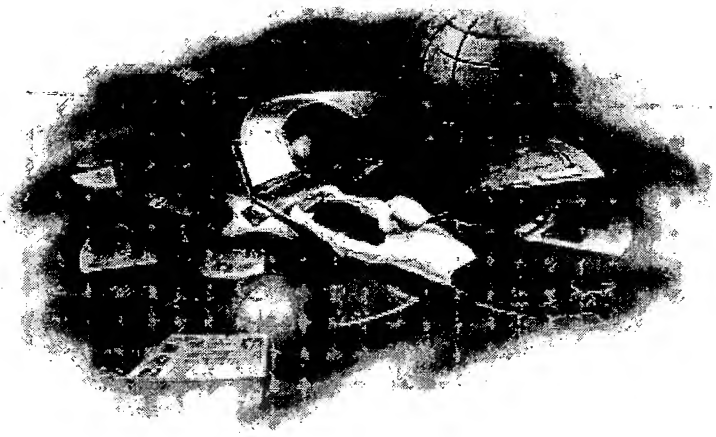
> Fast Roaming
- High density = Frequent roaming
- Minimizes latency to maintain Multi-media application performance



The Australian Stock Exchange is on board too.

Cisco can not match this performance!

...Nortel Creates Next Generation WLAN



WLAN 2202 Mobile Adapter
WLAN 2202-S Mobile Adapter for SIAC

Product Requirement Document

Revision 1.3.1

Removed from 2225/2202 PRD to be stand alone PRD

For fast track schedule

William R. Douglass

Revision History

Rev.	Responsible Persen	Description
1.0	Bill Douglass	Creation of the document
1.2.0	Lisa Schwartz	SIAC Requirements added
1.3.0	Lisa Schwartz	SIAC Requirements Updated with Preetam Sirur, John Brancato, Bob Friday and Account Teams at Nortel and Airespace responsible for SIAC.
1.3.1	Lisa Schwartz	Power Consumption Table Added

Table of Contents

Mobile Adapter 2202

1. WLAN 2202 Mobile Adapter

1. Introduction

The NORTEL NETWORKS WLAN 2202 is an IEEE 802.11a/b/g standard compatible Card Bus PC Card, which supports high data rate up to 54Mbps (for 802.11a) or 11Mbps (for 802.11b) or 54Mbps (for 802.11g) over the Ethernet speed. It is easy to install on various devices, which has Card Bus interface. The software supports most of O.S. for operation. The automatic fallback feature is to secure the operation with lower data rate under the specific noisy environment.

1.1 Scope

This document describes the hardware and software specification for the NORTEL NETWORKS WLAN 2202.

1.2 Product Features

- All current features in v.1.3 for 2201
- High speed for wireless LAN connection, 54 Mbps data rate for 802.11a with enhanced "turbo mode" for extended range or speed up to 108 Mbps. 11Mbps data rate for 802.11b and 54Mbps data rate for 802.11g
- Support Super G mode
- Support seamless roaming within the IEEE 802.11a or 802.11b or 802.11g WLAN infrastructure.
- Configuration utility
- WME
- Auto fallback data rate under noisy environment.
- Adjustable power levels for cell sizing on 802.11a/b/g
- Wireless data encryption with 64, 128, 152 bit encryption for security.
- Built-in dual diversity antenna
- Firmware upgrade-able by only changing driver.

1.3 Applications

- Wireless multimedia.
- Wireless office for extension Ethernet range.
- Mobile networking for notebook PC, PDA, Web Pad or Wireless Gateway Build-in Application.

2. Software

3.1 Operating System Support

- All current features in v.1.3 for 2201
- Windows 98SE Windows ME , Windows 2000, Windows XP, Windows NT4.0 , and MAC OS 9&10

3.2 Security

- Wired Equivalent Privacy (WEP) supports modes that have 40, 104, and 128 bit keys. With the concatenation of the 24 bit IV, these keys become 64, 128, 152 bit. These supported modes and keys will be available through Windows network properties
- WPA/TKIP
- AES
- WAPI for China

3.3 Configuration Utility

- An Utility to set SSID, WEP key and dynamically view configuration and statistics

3. Appearance

Power LED_0 (Green)	Network LED_1 (Green)	Meaning	Comments
Slow-rate blink	OFF	Power save mode (default from power up or reset)	
ON	OFF	Awake	The hardware automatically enter this state after exit from power save mode before any other activity. Change from power save mode to this state might not be visible on the LEDs if the software assumes control of the LED blinking by writing to the PCI configuration register
Alternate blink	Alternate blink	Looking for network association	Power LED goes ON; Network LED is OFF; then Power LED goes OFF and Network LED goes ON
Slow-rate blink	Slow-rate blink	Associated or joint with network; no activity	
Fast-rate blink	Fast-rate blink	Associated or joint with network; blink rate increases with activity on the network over the air or locally on the network device based on setting of the PCI configuration register	
OFF	OFF	No power applied to the card	

4. Specifications

802.11a Radio

- Frequency Band: 2.4 ~ 2.5GHz
  5.15 ~ 5.25GHz (lower band) for US/Canada, Japan
  5.25 ~ 5.725GHz (middle band) for US/Canada
  5.725~5.850GHz (higher band)
- Modulation TYPE: OFDM, CCK
- Operating Channels: IEEE 802.11a compliant
  8 channels in 802.11a standard mode (US, Canada)
  3 channels in turbo mode (US, Canada)
  4 channels (Japan)
  IEEE 802.11b compliant
- Operating Voltage: 3.0V ~ 3.6V
- Transmitted Power: *See Table1*
- Rates/Sensitivity/Allowable Path Loss: *See the Table 2.*
- Mechanical spec.
  - CardBus Type II

Country Approvals	U.S. FCC, Canada IC	
	Japan TELEC	
	Europe ETSI	For countries which accept .11a as of July 2002
Safety Approvals	CE Mark (EN60950)	Required to ship into Europe
	C-UL	OEM customer requirement (Siemens)
Emissions / Susceptibility	FCC Part 15	Subpart B, Class B digital device, 15.205, 15.209, 15.401-407
	IC RSS 210	ICES-102, ICES-003
	EN 301 893	Harmful interference
	EN 301 489-17	EMC
	EN 55022, CISPR Class B	Emissions
Environmental	Temperature Operational	-30 to 75 °C
	Temperature Storage	-65 to 150 °C
	Altitude Operational	0 to 10,000 feet
	Altitude Storage	0 to 15,000 feet
	Transport	Air-transport In un-pressurized cargo holds
	ESD	Cardbus Standard to 15 kV
	Shock and Vibration	Cardbus Standard to 15 Gs
	Humidity	5 ~ 90% and must be non-condensing
Certifications	WiFi; WQHL	

1.1 Table 1: Modulation Scheme and Transmit Power

Modulation Rate	Output Power 2.4-2.5GHz	Output Power 5.15-5.25GHz	Output Power 5.25-5.725GHz	Output Power 5.725-5.850GHz
802.11b (1Mbps)	18	NA	NA	NA
802.11b (2Mbps)	18	NA	NA	NA
802.11b (5.5Mbps)	18	NA	NA	NA
802.11b (11Mbps)	18	NA	NA	NA
802.11a (6Mbps)	NA	17	17	16
802.11a (9Mbps)	NA	17	17	16
802.11a (12Mbps)	NA	17	17	16
802.11a (18Mbps)	NA	17	17	16
802.11a (24Mbps)	NA	17	17	16
802.11a (36Mbps)	NA	15	15	15
802.11a (48Mbps)	NA	14	14	12
802.11a (54Mbps)	NA	13	13	10
Turbo (12Mbps)	NA	16	16	16
Turbo (18Mbps)	NA	16	16	16
Turbo (24Mbps)	NA	16	16	16
Turbo (36Mbps)	NA	16	16	16
Turbo (48Mbps)	NA	16	16	16
Turbo (72Mbps)	NA	15	15	15
Turbo (96Mbps)	NA	14	14	12
Turbo (108Mbps)	NA	13	13	10

1.1.1 Table 2: Typical Range at Which Frame (1000 Bytes PDUs) Packet Error Rate=10%

Modulation Rate	Receiver Sensitivity 5.15-5.25GHz (dBm)	Receiver Sensitivity 5.25-5.35GHz (dBm)	Receiver Sensitivity 5.725-5.85GHz (dBm)
802.11a – 6Mbps	-88	-88	-85
802.11a – 9Mbps	-86	-86	-83
802.11a – 12Mbps	-85	-85	-82
802.11a – 18Mbps	-83	-83	-80
802.11a – 24Mbps	-80	-80	-77
802.11a – 36Mbps	-76	-76	-73
802.11a – 48Mbps	-71	-71	-68
802.11a – 54Mbps	-68	-68	-65

1.2 Table 1A. Power Consumption

2202 MA Measured Power Consumption

Item	Frequency	54Mbps	11A mode TX Power Consumption 48Mbps 36Mbps 24Mbps 18Mbps				12Mbps	9Mbps	6Mbps
1	5180MHZ	453mA	464mA	481mA	502mA	502mA	502mA	502mA	502mA
		1495mW	1531mW	1587mW	1657mW	1657mW	1657mW	1657mW	1657mW
	5500MHZ	505mA	517mA	562mA	585mA	585mA	585mA	585mA	585mA
		1667mW	1706mW	1855mW	1931mW	1931mW	1931mW	1931mW	1931mW
	5800MHZ	530mA	539mA	570mA	593mA	593mA	593mA	593mA	593mA
		1749mW	1779mW	1881mW	1957mW	1957mW	1957mW	1957mW	1957mW
2	5180MHZ	468mA	477mA	498mA	524mA	524mA	524mA	524mA	524mA
		1544mW	1574mW	1643mW	1729mW	1729mW	1729mW	1729mW	1729mW
	5500MHZ	522mA	551mA	581mA	604mA	604mA	604mA	604mA	604mA
		1723mW	1818mW	1917mW	1993mW	1993mW	1993mW	1993mW	1993mW
	5800MHZ	554mA	570mA	624mA	650mA	650mA	650mA	650mA	650mA
		1828mW	1881mW	2059mW	2145mW	2145mW	2145mW	2145mW	2145mW
3	5180MHZ	450mA	467mA	495mA	510mA	510mA	510mA	510mA	510mA
		1485mW	1541mW	1634mW	1683mW	1683mW	1683mW	1683mW	1683mW
	5500MHZ	479mA	500mA	532mA	565mA	565mA	565mA	565mA	565mA
		1581mW	1650mW	1756mW	1865mW	1865mW	1865mW	1865mW	1865mW
	5800MHZ	519mA	544mA	589mA	632mA	632mA	632mA	632mA	632mA
		1713mW	1795mW	1944mW	2086mW	2086mW	2086mW	2086mW	2086mW
4	5180MHZ	449mA	461mA	477mA	505mA	505mA	505mA	505mA	505mA
		1482mW	1521mW	1574mW	1667mW	1667mW	1667mW	1667mW	1667mW
	5500MHZ	488mA	495mA	526mA	569mA	569mA	569mA	569mA	569mA
		1610mW	1634mW	1736mW	1878mW	1878mW	1878mW	1878mW	1878mW
	5800MHZ	509mA	522mA	560mA	591mA	591mA	591mA	591mA	591mA
		1680mW	1723mW	1848mW	1950mW	1950mW	1950mW	1950mW	1950mW
5	5180MHZ	456mA	462mA	471mA	501mA	501mA	501mA	501mA	501mA
		1505mW	1525mW	1554mW	1653mW	1653mW	1653mW	1653mW	1653mW
	5500MHZ	482mA	489mA	512mA	537mA	537mA	537mA	537mA	537mA
		1591mW	1614mW	1690mW	1772mW	1772mW	1772mW	1772mW	1772mW
	5800MHZ	493mA	509mA	538mA	561mA	561mA	561mA	561mA	561mA
		1627mW	1680mW	1775mW	1851mW	1851mW	1851mW	1851mW	1851mW

2202 MA Measured Power Consumption

Item	Frequency	54Mbps	11G mode TX Power Consumption 48Mbps 36Mbps 24Mbps 18Mbps				12Mbps	9Mbps	6Mbps
1	2412MHZ	450mA	452mA	463mA	472mA	472mA	472mA	472mA	472mA
		1485mW	1492mW	1528mW	1558mW	1558mW	1558mW	1558mW	1558mW
	2472MHZ	450mA	450mA	458mA	476mA	476mA	476mA	476mA	476mA
		1485mW	1485mW	1511mW	1571mW	1571mW	1571mW	1571mW	1571mW
2	2412MHZ	470mA	473mA	480mA	489mA	489mA	489mA	489mA	489mA
		1551mW	1561mW	1584mW	1614mW	1614mW	1614mW	1614mW	1614mW
	2472MHZ	473mA	476mA	484mA	496mA	496mA	496mA	496mA	496mA
		1561mW	1571mW	1597mW	1637mW	1637mW	1637mW	1637mW	1637mW
3	2412MHZ	449mA	449mA	458mA	470mA	470mA	470mA	470mA	470mA
		1482mW	1482mW	1511mW	1551mW	1551mW	1551mW	1551mW	1551mW
	2472MHZ	447mA	450mA	456mA	468mA	468mA	468mA	468mA	468mA
		1475mW	1485mW	1505mW	1544mW	1544mW	1544mW	1544mW	1544mW
4	2412MHZ	435mA	435mA	441mA	448mA	448mA	448mA	448mA	448mA
		1436mW	1436mW	1455mW	1478mW	1478mW	1478mW	1478mW	1478mW
	2472MHZ	438mA	441mA	452mA	459mA	459mA	459mA	459mA	459mA
		1445mW	1455mW	1492mW	1515mW	1515mW	1515mW	1515mW	1515mW
5	2412MHZ	472mA	474mA	481mA	486mA	486mA	486mA	486mA	486mA
		1558mW	1564mW	1587mW	1604mW	1604mW	1604mW	1604mW	1604mW
	2472MHZ	469mA	471mA	476mA	486mA	486mA	486mA	486mA	486mA
		1548mW	1554mW	1571mW	1604mW	1604mW	1604mW	1604mW	1604mW

2202 MA Measured Power Consumption

Item	Frequency	11Mbps short	11B mode TX Power Consumption 11Mbps long 5.5Mbps short 5.5Mbps long			2Mbps short	2Mbps long	1Mbps long
1	2412MHZ	446mA	449mA	446mA	449mA	446mA	449mA	449mA
		1472mW	1482mW	1472mW	1482mW	1472mW	1482mW	1482mW
	2472MHZ	472mA	472mA	472mA	472mA	472mA	472mA	472mA
		1558mW	1558mW	1558mW	1558mW	1558mW	1558mW	1558mW
2	2412MHZ	470mA	470mA	470mA	470mA	470mA	470mA	470mA
		1551mW	1551mW	1551mW	1551mW	1551mW	1551mW	1551mW
	2472MHZ	484mA	490mA	484mA	490mA	484mA	490mA	490mA
		1597mW	1617mW	1597mW	1617mW	1597mW	1617mW	1617mW
3	2412MHZ	446mA	446mA	446mA	446mA	446mA	446mA	446mA
		1472mW	1472mW	1472mW	1472mW	1472mW	1472mW	1472mW
	2472MHZ	456mA	456mA	456mA	456mA	456mA	456mA	456mA
		1505mW	1505mW	1505mW	1505mW	1505mW	1505mW	1505mW
4	2412MHZ	433mA	439mA	433mA	433mA	433mA	433mA	433mA
		1429mW	1449mW	1429mW	1429mW	1429mW	1429mW	1429mW
	2472MHZ	438mA	448mA	438mA	448mA	438mA	448mA	448mA
		1445mW	1478mW	1445mW	1478mW	1445mW	1478mW	1478mW
5	2412MHZ	479mA	479mA	479mA	479mA	479mA	479mA	479mA
		1581mW	1581mW	1581mW	1581mW	1581mW	1581mW	1581mW
	2472MHZ	479mA	479mA	479mA	479mA	479mA	479mA	479mA
		1581mW	1581mW	1581mW	1581mW	1581mW	1581mW	1581mW

2202 MA Measured Power Consumption

Item	Frequency	54Mbps	11A mode RX Power Consumption 48Mbps	36Mbps	24Mbps	18Mbps	12Mbps	9Mbps	6Mbps
1	5180MHZ	262mA	262mA	262mA	262mA	262mA	262mA	262mA	262mA
		865mW	865mW	865mW	865mW	865mW	865mW	865mW	865mW
	5500MHZ	262mA	262mA	262mA	262mA	262mA	262mA	262mA	262mA
		865mW	865mW	865mW	865mW	865mW	865mW	865mW	865mW
	5800MHZ	262mA	262mA	262mA	262mA	262mA	262mA	262mA	262mA
		865mW	865mW	865mW	865mW	865mW	865mW	865mW	865mW
2	5180MHZ	259mA	259mA	259mA	259mA	259mA	259mA	259mA	259mA
		855mW	855mW	855mW	855mW	855mW	855mW	855mW	855mW
	5500MHZ	259mA	259mA	259mA	259mA	259mA	259mA	259mA	259mA
		855mW	855mW	855mW	855mW	855mW	855mW	855mW	855mW
	5800MHZ	259mA	259mA	259mA	259mA	259mA	259mA	259mA	259mA
		855mW	855mW	855mW	855mW	855mW	855mW	855mW	855mW
3	5180MHZ	264mA	264mA	264mA	264mA	264mA	264mA	264mA	264mA
		871mW	871mW	871mW	871mW	871mW	871mW	871mW	871mW
	5500MHZ	264mA	264mA	264mA	264mA	264mA	264mA	264mA	264mA
		871mW	871mW	871mW	871mW	871mW	871mW	871mW	871mW
	5800MHZ	264mA	264mA	264mA	264mA	264mA	264mA	264mA	264mA
		871mW	871mW	871mW	871mW	871mW	871mW	871mW	871mW
4	5180MHZ	267mA	267mA	267mA	267mA	267mA	267mA	267mA	267mA
		881mW	881mW	881mW	881mW	881mW	881mW	881mW	881mW
	5500MHZ	267mA	267mA	267mA	267mA	267mA	267mA	267mA	267mA
		881mW	881mW	881mW	881mW	881mW	881mW	881mW	881mW
	5800MHZ	267mA	267mA	267mA	267mA	267mA	267mA	267mA	267mA
		881mW	881mW	881mW	881mW	881mW	881mW	881mW	881mW
5	5180MHZ	269mA	269mA	269mA	269mA	269mA	269mA	269mA	269mA
		888mW	888mW	888mW	888mW	888mW	888mW	888mW	888mW
	5500MHZ	269mA	269mA	269mA	269mA	269mA	269mA	269mA	269mA
		888mW	888mW	888mW	888mW	888mW	888mW	888mW	888mW
	5800MHZ	269mA	269mA	269mA	269mA	269mA	269mA	269mA	269mA
		888mW	888mW	888mW	888mW	888mW	888mW	888mW	888mW

2202 MA Measured Power Consumption

Item	Frequency	54Mbps	11G mode RX Power Consumption 48Mbps 36Mbps 24Mbps 18Mbps				12Mbps	9Mbps	6Mbps
1	2412MHZ	267mA	267mA	267mA	267mA	267mA	267mA	267mA	267mA
		881mW	881mW	881mW	881mW	881mW	881mW	881mW	881mW
	2472MHZ	267mA	267mA	267mA	267mA	267mA	267mA	267mA	267mA
		881mW	881mW	881mW	881mW	881mW	881mW	881mW	881mW
2	2412MHZ	266mA	266mA	266mA	266mA	266mA	266mA	266mA	266mA
		878mW	878mW	878mW	878mW	878mW	878mW	878mW	878mW
	2472MHZ	266mA	266mA	266mA	266mA	266mA	266mA	266mA	266mA
		878mW	878mW	878mW	878mW	878mW	878mW	878mW	878mW
3	2412MHZ	267mA	267mA	267mA	267mA	267mA	267mA	267mA	267mA
		881mW	881mW	881mW	881mW	881mW	881mW	881mW	881mW
	2472MHZ	267mA	267mA	267mA	267mA	267mA	267mA	267mA	267mA
		881mW	881mW	881mW	881mW	881mW	881mW	881mW	881mW
4	2412MHZ	270mA	270mA	270mA	270mA	270mA	270mA	270mA	270mA
		891mW	891mW	891mW	891mW	891mW	891mW	891mW	891mW
	2472MHZ	270mA	270mA	270mA	270mA	270mA	270mA	270mA	270mA
		891mW	891mW	891mW	891mW	891mW	891mW	891mW	891mW
5	2412MHZ	274mA	274mA	274mA	274mA	274mA	274mA	274mA	274mA
		904mW	904mW	904mW	904mW	904mW	904mW	904mW	904mW
	2472MHZ	274mA	274mA	274mA	274mA	274mA	274mA	274mA	274mA
		904mW	904mW	904mW	904mW	904mW	904mW	904mW	904mW

2202 MA Measured Power Consumption

Item	Frequency	11Mbps short	11B mode RX Power Consumption 11Mbps long 5.5Mbps short 5.5Mbps long			2Mbps short	2Mbps long	1Mbps long
1	2412MHZ	246mA	246mA	246mA	246mA	246mA	246mA	246mA
		812mW	812mW	812mW	812mW	812mW	812mW	812mW
	2472MHZ	246mA	246mA	246mA	246mA	246mA	246mA	246mA
		812mW	812mW	812mW	812mW	812mW	812mW	812mW
2	2412MHZ	246mA	246mA	246mA	246mA	246mA	246mA	246mA
		812mW	812mW	812mW	812mW	812mW	812mW	812mW
	2472MHZ	246mA	246mA	246mA	246mA	246mA	246mA	246mA
		812mW	812mW	812mW	812mW	812mW	812mW	812mW
3	2412MHZ	248mA	248mA	248mA	248mA	248mA	248mA	248mA
		818mW	818mW	818mW	818mW	818mW	818mW	818mW
	2472MHZ	248mA	248mA	248mA	248mA	248mA	248mA	248mA
		818mW	818mW	818mW	818mW	818mW	818mW	818mW
4	2412MHZ	246mA	246mA	246mA	246mA	246mA	246mA	246mA
		812mW	812mW	812mW	812mW	812mW	812mW	812mW
	2472MHZ	246mA	246mA	246mA	246mA	246mA	246mA	246mA
		812mW	812mW	812mW	812mW	812mW	812mW	812mW
5	2412MHZ	253mA	253mA	253mA	253mA	253mA	253mA	253mA
		835mW	835mW	835mW	835mW	835mW	835mW	835mW
	2472MHZ	253mA	253mA	253mA	253mA	253mA	253mA	253mA
		835mW	835mW	835mW	835mW	835mW	835mW	835mW

5. Radios

Atheros Chipsets AR5115 radio, MAC 5213, CB42 reference design, with Atheros 3.1 driver.

802.11B/G WIRELESS RADIO

- Radio: 802.11g

2400 ~ 2483.5 MHz (for US, Canada)
2400 ~ 2483.5 MHz (for ETSI, Japan)
802.11b
2400 ~ 2483.5 MHz (for US, Canada)
2400 ~ 2483.5 MHz (for ETSI)
2400 ~ 2497 MHz (For Japan)

- Operating Channels: 802.11G

11 channels in base mode (US, Canada)
13 channels (ETSI, Japan)
802.11b
11 channels in base mode (US, Canada)
13 channels (ETSI)
14 channels (Japan)

- Radio Technology: Direct Sequence Spread Spectrum (DSSS) / Orthogonal Frequency Division Multiplexing (OFDM)
- Date Rate: 1/2/5.5/11 (11b) Mbps 6/9/12/18/24/36/48/54 Mbps (11g)
- Media Access Protocol: CSMA/CA with ACK
- Output Power: Configurable Output Power with up to 65 mW per table 3
- Receive Sensitivity as per table 4
- Antenna type Fixed Antenna
- Antenna gain 1.5 dBi
- Radio On/OF: Radio on/off control by utility

1.3 Table 3: Modulation Scheme and Transmit Power3

Rate	**Maximum Output Power 2412 MHz (dBm)**	**Maximum Output Power 2417 ~ 2457 MHz (dBm)**	**Maximum Output Power 2462 MHz (dBm)**
802.11g – 6Mbps	17	17	17
802.11g – 9Mbps	17	17	17
802.11g – 12Mbps	17	17	17
802.11g – 18Mbps	17	17	17
802.11g – 24Mbps	17	17	17
802.11g – 36Mbps	15.5	15.5	15.5
802.11g – 48Mbps	13.5	13.5	13.5
802.11g – 54Mbps	11.5	11.5	11.5
802.11b –1 Mbps	18	18	18

802.11b –2 Mbps 18 18 18
802.11b – 5.5Mbps 18 18 18
802.11b – 11 Mpbs 18 18 18
Notes for tables:
* The output power is measured at the Hirose connector with the RMS (root mean square, or average) power meter.
* The maximum transmit power in Table3 is determined by both (1) 10% packet error rate at 3 dB above 802.11b/g rate dependent sensitivity and (2) 802.11b/g spectrum mask limit.
* The maximum transmit power may be lowered by regulatory (FCC, ETSI, etc) EIRP (effective isotropic radiated power) limit.
* The maximum transmit power may be lowered by regulatory (FCC, ETSI, etc) restricted limit depending on the RF shielding of the platform in which the model installed.
3 MB22g FCC limits for reference: 2412 MHz 14 dBm, 2417 MHz 16 dBm, 2422-2447 MHz 18 dBm , 2452 MHz 17 dBm, 2457 MHz 15 dBm, 2462 MHz 13 dBm

1.3.1 Table 4: Typical Range at Which Frame (1000 Bytes PSDUs) Error Rate=10%

Rate
Sensitivity
2412 ~ 2484 GHz
(dBm)
802.11g – 6Mbps -88
802.11g – 9Mbps -87
802.11g – 12Mbps -86
802.11g – 18Mbps -85
802.11g – 24Mbps -81
802.11g – 36Mbps -77
802.11g – 48Mbps -72
802.11g – 54Mbps -70
802.11b –1 Mbps -93
802.11b –2 Mbps -90
802.11b – 5.5Mbps -90
802.11b – 11 Mpbs -87

6. Mobile Adaptor 2202-S SIAC Client Requirements

The Mobile Adapter Driver is a custom service Nortel Networks is performing for the SIAC Customer. Due to multiple feature requests needed to satisfy the Customer's requirements, custom client software needs to be developed, tested for Quality Assurance and performance, and validated as part of the integrated system within the trading floor environment. This effort will be required for the features listed below. The WLAN system comprises the custom client device and the WLAN switch and APs. The Mobile Adapter Driver shall support the following requirements.

This unit will be shipped with its own CD driver for SIAC and in its own packaging.

2202-S Client Requirements

Attribute	Required and In Developme	Strongly Desired and POI	Optional and for Future	Comments
Fast roaming in a pico cell environment	X			Roaming relates to the ability of the mobile unit to seamlessly transition its connectivity from one access port (AP) to another with packet delays as measured by IxChariot not exceeding 100 ms with all required security features enabled including the ability to recover form wired side failures.
Load Balancing	X			Load balancing relates to the ability of the mobile unit (MU) to roam to other access ports when several mobile units are concentrated in one area, they are distributed between the access ports covering that area such that no access port has a disproportionate share of mobile units attached to it.
Security Mechanism	X			The security mechanism must support WPA with TKIP and 802.1x authentication
Variable Client Receive Sensitivity	X			This parameter should be settable via registry settings or via the GUI to ensure optimum Pico-cell performance
Variable Client Transmit Power	X			This parameter should be settable via registry settings or via the GUI to ensure optimum Pico-cell performance.
Support Single Data Rate Configuration	X			2.6 Bug Fix: Support the ability to function at a single selected data rate e.g. 36 Mbps
Client Power Management	X			2.7 Power management relates to the ability of the MU to use the minimum transmit power required to sustain the required throughput rate when in use, and to be able to sleep when not in use, thereby minimizing noise and interference and maximizing battery life (power save mode) variation of modes to save battery life.
Customized Client API	X			The driver must provide an API to enable an applet to extract relevant radio information and for Statistical retrieves resident to the mobile devices
Support for the new UNII channels		X		This should be provided in the 3.1.x version of the standard Atheros Code. 2.9
Support for non PicoCell networks	X			2.3
Backward Compatible	X			The driver must be delivered in such a format that is downloadable for the purposes of driver upgrades, as well as supporting fallbacks to previous versions.
Uninstall utility	X			The driver must provide an uninstall utility that completely uninstalls the previously installed driver and allows a clean installation of the current driver, alternately the driver must be delivered in such a format that it completely over-writes the previously installed.

2202-S Client Requirements, Cont'd

Attribute	Required and In Developm	Strongly Desired and POI	Optional and for Future	Comments
Multiple OS Support	X			Windows2000, WindowsXP, and Windows CE.Net 4.2 (NYSE custom PDA running Win CE.NET v4.2). Additional operating systems support for CE.Net v5.0, Win XP Embedded, and Linux is beyond these three and is understood to require a change order request and would be billed as an additional charge to NYSE.
WPA2 Optimized Handoff Extension	X			Currently, with WPA2 opportunistic PMK Caching, after each hand-off the client will attempt to short-cut the authentication process by providing its PMKID in the new association request. This will cause the 2270 to initiate the key exchange that will generate a new PTK and GTK. The WPA2 Optimized Handoff extension will eliminate the need to re-key after every association by allowing the client to re-use its existing PTK and GTK. The Funk supplicant and the Intelligraphics custom client will also have to support this feature, and this must be planned separately. Pat Calhoun has initiated a discussion with Funk Software to get them to add this feature in their supplication and Intelligraphics. (3) requirements for optimized handoff: 1. WPA2 2. PMK Caching 3. WARP – intrprepration of standard so that you have better ways to handle re-keying which is bad for the system. **Affects: Client, Appliance** - Supported from mgmt. config to WPA2
Minimize inter-switch hand-offs	X			The SIAC network design is such that every other AP is connected to a different switch. It would be preferable to reduce the occurrences of inter-switch hand-offs in order to decrease hand-off latency. Both on Appliance, Driver
Support for WPA2	X			WPA2 is now shipping as an experimental feature in 2.1 and has been through two plug fest testing events. Airespace tested against the Funk supplicant and the Atheros driver. This feature will be provided to SIAC once. This feature will be provided with the 2.1 code merge (see 2.10) AES in hardware support.
Switch Handoff Optimizations				To optimize the Inter-Mobility group handoff and also increase the current scalability of mobility a feature has been proposed to have the client via the Custom client driver provide the switch-ID of where it was attached, to the new switch (Intra or Inter-mobility Group) that it roams to. This would enable the "new" switch to send a unicast packet (instead of a groupcast or broadcast packet) to the previous client switch. This also removes the current limitation of sending the groupcast to all members of a mobility group. This feature request is currently being designed and developed for deployment in the planned release for SIAC.

11. RF Requirements for SIAC Mobile Adaptor 2202-S

The SIAC wireless network design will incorporate the 5 GHz 802.11a frequency bands and utilize up to 23 channels in a pico-cell design (when available by the FCC). The design is intended to fulfill the following functional requirements:

- Be highly reliable.
- Support roaming.
- Provide no single point of failure.
- Provide no degradation of performance due to a single failure.
- Be scalable and allow for future growth (e.g., new wireless protocols, dual band operation).
- Provide a very high degree of security (not necessarily requiring a standards based solution).
- Support extensive manageability and monitoring.
- Provide high bandwidth performance with minimal latency.
- Support seamless connectivity for highly mobile users.

A full disclosure of the radio requirements pertaining to a standard GA release is out of scope of this document. Only unique RF requirements for SIAC are discussed.

According to technology assessment and studies performed by SIAC and NYSE, the desired RF design to support the dense and redundant environment of the NYSE trading floor is a "Pico-Cell" design. This term refers to a cellular design where channelized coverage cells are reduced in size to the extent that the throughput requirements of the dense user community can be satisfied.
Over all area of coverage by the WDS network consists of approximately 45,000 sq. ft. at the trading floor and additional 40000 sq. ft. of service area adjacent to the trading floor.
Number of wireless clients in the WDS network is 1500 users and 15% additional mobile devices deployed for monitoring and management purposes.

The cell design will account for occasional dense user clusters of 4.5 square feet per user, while guarantying each user the basic throughput and latency for which the system was designed. Further, for densities greater than 4.5 square feet per user, the system shall degrade gracefully.
Cell design should provide inherent RF coverage redundancy to account for single device failure scenarios. RF coverage redundancy will ensure that a single Access Point (AP) failure will not result in performance degradation. Users within the coverage of this Access Point must not experience any data loss, throughput, or latency degradation.

RF Requirements

Attribute	Required and In Development	Strongly Desired and POI	Optional and for Future Release	Comments
UNII Support		X		In order to support the higher mid-UNII bands, we must perform RADAR detection on these bands. However, it appears that the FCC may be making changes in which bands require RADAR detection. Current implementation will perform RADAR detection on all channels.

END OF DOCUMENT

Using picocells to build high-throughput 802.11 networks

In a typical indoor 802.11 wireless network, a single access point can cover 2500 to 10,000 square feet. Picocells are substantially smaller RF coverage areas and are used to provide high data throughput for dense wireless terminals/appliances by minimizing the amount of bandwidth that is shared among wireless users.

By Gregory Davi

In a typical indoor 802.11 wireless network, a single access point can cover 2500 to 10,000 square feet (based on typical access point placement, which is normally 50-100 feet apart). Picocells are substantially smaller RF coverage areas—on the order of 150 to 1000 square feet (cells on the order of 10-35 feet in diameter). They are used to provide high data throughput for dense wireless terminals and appliances by minimizing the amount of bandwidth that is shared among wireless users. A sample application for picocells would be a sporting arena, lecture hall, dense cubicle farm, or the trading floor of a stock exchange, where hundreds of wireless users require simultaneous high-bandwidth wireless services while confined within a localized space.

Creating a single picocell is relatively easy. However, it is difficult to deploy large numbers of non-overlapping picocells in a tightly packed space.

Designing a picocell wireless network

The basic design elements available in creation of picocells are radio transmit power control and receiver sensitivity control at the wireless access point (AP) and a mobile station (i.e. "client").

The primary issues associated with picocell design are:

- RF multipath and scattering.
- 802.11 protocol non-ideal results.
- number of available channels.
- high-gain antennas.
- balancing of RF link symmetry.
- coverage redundancy.
- user performance and fairness.

The coverage area of an AP can be reduced by decreasing the RF link budget (transmit power and receiver sensitivity) of the AP and the mobile station. In addition to controlling the link budget, the effect of co-channel interference and adjacent-channel RF interference must be dealt with before bringing APs and clients closer together. The strength of interference between cells will affect the quality of the RF link and the throughput of the cell(s) due to 802.11's built-in interference mitigation: carrier-sense multiple access (CSMA).

Picocell creation

Generally the size of an RF coverage cell, with the center being the AP, is based on the maximum capabilities of the radio design of the access point and the client in terms of transmit power, receiver sensitivity, antenna gain and RF environment. Typical 2.4 GHz and 5 GHz transmit power, which is regulated by the Federal Communications Commission (FCC), is around +17 to +30 dBm (50 mW to 1 W). Typical radio receiver demodulation maximum sensitivity is around –90 dBm for base data rate modulations and all data packet headers for 802.11a/b/g. Antenna gain maximums are limited by the FCC.

Transmit power control and receiver sensitivity control—Adjusting transmitter power and receiver sensitivity is one method to create a picocell. These parameters may be adjusted via hardware or software. Software adjustments of hardware can be made in terms of transmitter power control, implemented in adjustable hardware amplifier feedback loops. Software adjustments of hardware receivers can be made by setting the receiver (at baseband demodulation) to immediately ignore the packet if it does not exceed a mini-

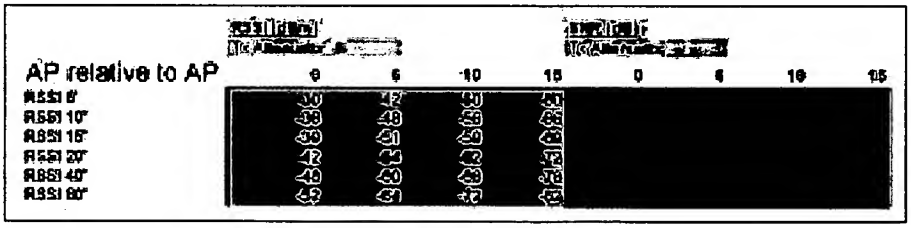


Table 1: General Empirical Results between Co-Channel APs (6dBi Antennas)

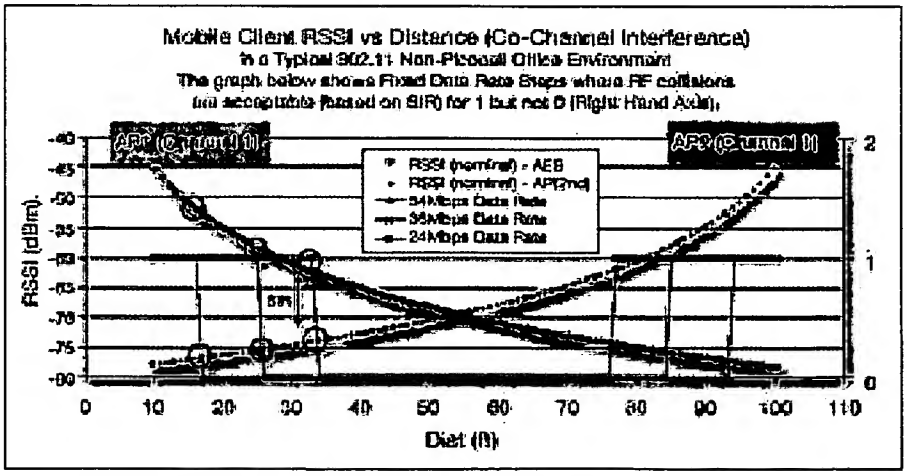


Figure 1a. Client perceived interference between co-channel APs.

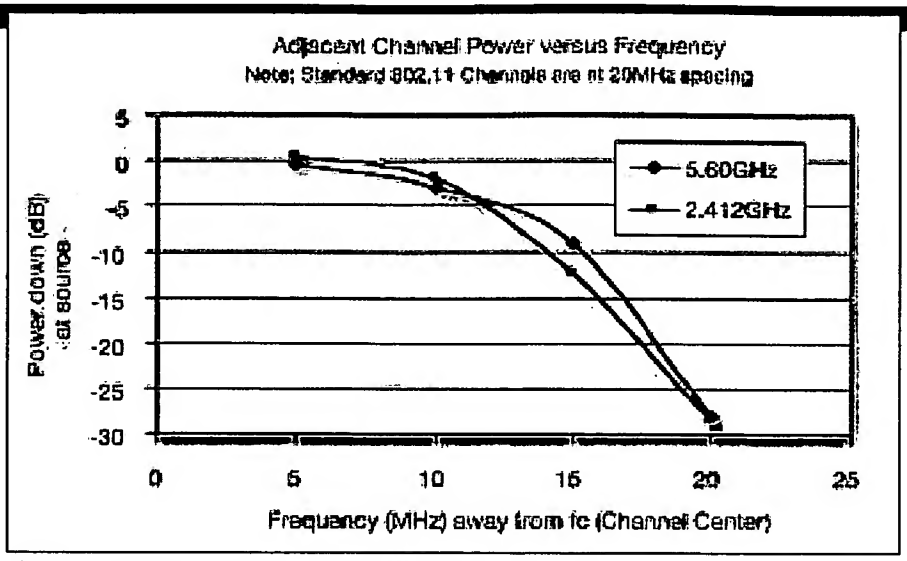


Figure 1b. Adjacent channel interference between co-channel APs.

mum signal-to-noise ratio (SNR) threshold.

Figure 1 is a typical ceiling-mounted relationship between APs, comparing attenuators with distance. The strength of the signal is quantified by the received signal strength intensity (RSSI).Table 1 is a typical ceiling-mounted relationship between APs (with no attenuators) and the co-channel and adjacent interference, as measured by signal-to-interference ratio (SIR), from the clients' perspective.

Special high-gain antennas—Special high-gain antennas can help control the area of RF coverage by focusing the main portion of energy on a particular area, thereby creating spatial diversity and more available bandwidth for other areas. Antenna gain is generally measured in terms of an antenna's 3 dB beamwidth in both the horizontal plane (azimuth) and the vertical plane (elevation) relative to an isotropic radiator. Typical 802.11 low-gain antennas are 2.2 to 6 dBi omnidirectional dipole\patch antennas with sizes in the range of 2 inches x 2 inches, but a high-gain antenna can be 2 to 10 times larger depending on the amount of directivity. Other types of modern antennas can use phased arrays or Multi-Input Multi-Output (MIMO) smart antenna technology to enhance directivity.

Design issues

Protocol reality (data rate and minimum SNR\SIR)—One key constraint in creation of picocells is the choice of data rate. The higher the data rate, the higher the SNR and SIR requirements for both the AP and client (see Figure 1).

Protocol reality (CSMA/CA)—All 802.11 packets have packet headers that are at the minimum data rate and have minimum SNR requirements (i.e. 802.11a is 6 dB SNR). When decoding a distant packet header on the same channel, the 802.11 protocol requires a radio (via CSMA/CA) to defer transmission of any packet, reducing its throughput. CSMA/CA constricts throughput of any 802.11 device because it will defer transmission if it "hears" a packet header. The RF reality mentioned above creates a strict limitation to the problem of spacing so that picocells sharing the same channel do not hear each other yet have enough SNR power to decode high date rates. Furthermore, the distance that the header can be heard compared to the data is far greater due to the data payload's high SNR requirement when >6 Mbps (see Figure 1). Receiver sensitivities, usually implemented in software, can make decisions to ignore packets on computation of header SNR below a user-defined threshold.

RF interference and cell overlap—Interference in a picocell is a critical attribute to be considered as the maximum density of APs and clients will be constrained by this. Interference is determined by the strength of same-channel or adjacent-channel RF power in a channel due to frequency and physical overlap. The strength of RF overlap is controlled by transmit power/ receiver sensitivity, antennas and number of channels.

Location of adjacent channels cannot necessarily be placed right next to each other. This results in a shuffling of channels to ensure that immediately adjacent channels do not overlap from one cell to another. Adjacent channels have about 30 dB worth of isolation, given all measurements are equal (see Figure 1 and 2).

Number of available channels—Another constraint that comes to bear is the number of channels available. The spacing density of reused channels is a function of the number of available channels. At this point in time, 802.11b has three channels (1, 6 and 11) available. 802.11a has a total of 23 channels with 12 standard channels (36,40,44,48,52,56,60,64,149,153,157,161) and 11 recently added channels (100, 104,108,112,116,120,124,128,132,136,140).

High-gain antennas—With regard to high-gain antennas, the directivity may help contain the focus of the main beam, but the moment that the energy hits any object, scattering occurs. Scattering (reflection, refraction or diffraction) off of walls, floors, and miscellaneous objects will result in some power loss. More importantly, the picocell designer will lose control over the direction of RF energy and hence, cell coverage, size and the possibility for one picocell on channel A to affect another picocell several cells away on channel A.

Balancing the symmetry of client and AP cell size—Balancing the symmetry of the AP-client RF link is also an important issue. For example, simple attenuation added between an AP and its antenna or reduction of AP transmit power will shrink the cell size. However, balancing of the RF link reduction ensures that the client receiver does not have a

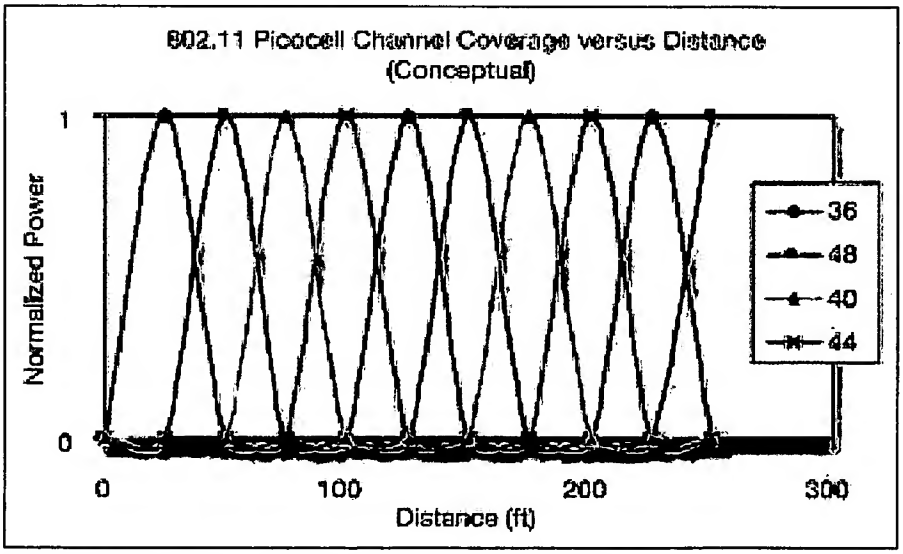


Figure 2. Adjacent channel interference spacing (repeating pattern).

much larger receiver range than the AP and vice versa. In this example, an AP with a reduction in transmit power and\or receiver sensitivity will not be able to see its co-channel AP, but the clients may be able to see the distant AP or other clients if it also does not have a reduction in power and receiver sensitivity. In addition, throughput will suffer due to collision avoidance CSMA/CA mechanism in the 802.11 protocol.

Given user density and throughput per user, basic equations that must be solved are cell size, SNR, and SIR requirements.

General equations:

Cell Size (estimate) = DataRateThroughput_per_Cell/ Throughput_per_client_Spec*Protocol_efficiency * space_per_client

Downlink dB Link Budget AP (estimate) = TxPower(AP) – Attenuator(AP) – Attenuator(Client) –Client(Noise Floor) > Data Rate SNR

Uplink dB Link Budget (estimate) = TxPower(Client) – Attenuator(Client) – Attenuator(AP) – AP(Noise Floor) > Data Rate SNR

SIR (estimate) = TxPower (AP/Client) – greater of [Co-Channel_Power(AP/Client), Power of adjacent-channel (AP/Client)]

Redundancy (to ensure network uptime)—Generally, because RF spectrum is a fixed resource, cell overlap is kept to a minimum. In some applications, redundancy may be considered. In this case, RF redundancy is the assurance that a coverage hole does not occur if an AP goes down. The spacing of access points and their antennas should not create a coverage hole if an AP or APs go down. The straightforward answer is to duplicate APs, one for one, on the same channel and duplicate network redundancy within the infrastructure. A less expensive approach would be to interlace APs with semi-overlapping coverage given wired side redundancy.

Fairness—In some applications, the effect of bandwidth sharing for more users under one AP relative to another AP with less users results in better user throughput under the less loaded AP. To ensure 100 percent balance among all users, one method—which can be a tricky task—is to equally balance all users based on the lowest performing user. Another option is to hard-fix all users at a minimum fixed link data rate and throughput.

Conclusion

Picocells are not as easy to create as back-of-the-napkin-engineering would lead you to believe. Some factors might require a decrease in picocell sizes, such as client density, throughput per user or total system capacity. Other factors typically result in an increase in picocell size and density, such as co-channel reuse, data rate SIR/SNR requirements, and the 802.11 CSMA/CA protocol mechanisms. Picocell creation is a delicate balancing act, requiring careful analysis of budgets, data rates, density, available channels, redundancy and throughput. However, when implemented appropriately, picocells can provide significant performance gains in many different types of indoor WLAN deployments. **RFD**

ABOUT THE AUTHOR

Gregory Davi is a systems engineer at Airespace,with numerous years of experience dealing with RF technology, including three patents pending on RF location tracking and one on RF security. He's authored several papers on wireless networking while at Airespace and in his previous role as -senior systems engineer at Metricom.